Interoperability Framework

Version 2.0 — 17 August 2007

National E-Health Transition Authority

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

Table of contents

Executive Summary

A national approach to interoperability is vital to the Australian e-health agenda. Interoperability contributes to enhanced healthcare delivery facilitating continuity of care and better decision making while delivering cost savings. Interoperability is also a state of readiness to deal with new technologies, clinical practices and changes in policies.

The NEHTA Interoperability Framework (IF) is a common reference point that provides guidance to business and IT experts in delivering interoperable e-health systems in Australia. This document presents the NEHTA Interoperability Framework (IF), version 2.0.

The IF 2.0 provides a number of updates to the NEHTA Interoperability Framework 1.0 [IF1.0]. While the IF1.0 was setting the direction for establishing a *shared understanding* of interoperability in Australian e-health, this version has a particular emphasis on highlighting the foundational role of the IF in *adopting* and *implementing* interoperability solutions and practices. These implementation concerns include:

- The use *of* the *interoperability concepts and patterns* in harmonising *enterprise modelling* and *enterprise architecture* activities within Australian e-health;
- The application of several *interoperability guidelines* to facilitate interoperability design, analysis and assessment;
- The introduction of appropriate *governance mechanisms* and organisational practices in support of interoperability readiness, such as *certification processes*, *enterprise architecture program* and *interoperability maturity program*.

The IF2.0 reflects an increasing level of maturity about interoperability, gained since the publication of the IF1.0, achieved in particular through:

- Discussions with key stakeholders in Australian e-health including representatives from the jurisdictions, standards organisations and vendor organisations;
- Further development of interoperability ideas, taking into account new technologies, clinical processes and business practices.

The aim of this version of the IF is to continue providing impetus towards better national e-health interoperability. This will be achieved through broadening the focus of this version, with the pragmatics of *implementing*, *adopting* and *nurturing* interoperability principles and practices in e-health projects.

The IF2.0 provides a number of *refinements* and *extensions* of the IF1.0, including:

- Several updates and additions to the existing family of *interoperability languages* needed to provide better expressiveness for enterprise architecture purposes;
- Identification of an initial[1] set of *interoperability patterns* as well as a number of new *categories* of interoperability patterns captured through analysis of several specific NEHTA and Jurisdictions e-health projects;
- Definition of a number of *interoperability goals* that crystallise key interoperability facets and facilitate definition, analysis and assessment of interoperability;

[1] These initial patterns were identified at the time of writing. This set will grow to accommodate new patterns that will be identified in the course of different e-health projects, both in the context of NEHTA work program and as part of jurisdictional and other efforts.

- The adoption of a small set of *enterprise architecture principles* and an *enterprise architecture methodology* to address interoperability problems within the scope of the national infrastructure with which NEHTA is tasked.

In addition, this version provides a set of *interoperability guidelines* in terms of:

- Approaches for *linking* interoperability *goals*, *patterns* and *concepts*;
- A *Conformance, Compliance and Accreditation* framework, for describing key roles, processes and policies needed to govern certification at organisational and national levels;
- An *Interoperability Maturity Model*, allowing e-health organisations to assess their existing interoperability parameters and define their interoperability improvement trajectories, towards ensuring optimum realisations of benefits associated with ICT.

This version has also identified a number of open issues and development milestones that need to be addressed in the next versions of the IF.

1 Introduction

This document presents the NEHTA Interoperability Framework (IF), version 2.0.

1.1 Purpose

The IF is a common reference point that provides guidance to business and IT experts in delivering interoperable e-health systems in Australia - while allowing for the evolutionary and emergent aspects of business, policy and technology.

This is achieved through:

- The separation of organisational, information and technical perspectives of e-health; this separation helps dealing with the diversity and complexity of the healthcare environment, facilitates dialogue between the respective stakeholders and encourages clarity of expression;
- The adoption of a commonly agreed set of interoperability concepts, as a foundation for an interoperability language, as well as interoperability patterns for each of the perspectives - developed based on the existing NEHTA, jurisdiction[2], and international experience; the interoperability language and patterns promote shared understanding about interoperability and serve as a common reference point for many specific e-health languages, facilitating their co-existence and linkages[3];
- A disciplined approach to delivering specifications, ensuring conformance of implementations to specifications and applying continual value assessment – to ensure longevity and sustainability.

The IF provides foundation principles for establishing or influencing enterprise architecture developments in Australian e-health as well as a basis for developing a national certification capability, addressing compliance, conformance and accreditation issues. In addition, this version of the IF comes with several guidelines and techniques in support of designing, developing and deploying interoperable e-health systems, such as interoperability assessment and an interoperability maturity model.

This IF version 2.0 is based on:

- The experience gained in using the interoperability concepts and patterns from the IF1.0 in the context of NEHTA work program;
- Feedback from many e-health experts from the Australian e-health community, including jurisdictions, different e-health organisations and national/international standards organisations, obtained through consultations, workshops or through electronic communication;
- New results obtained from further development of interoperability related themes within NEHTA, in particular in the areas of enterprise architecture, the interoperability maturity model and e-health certification.

[2] In Australian health jargon, the term 'jurisdiction' refers to individual State, Territory and Commonwealth health entities and their clinician and governance structures.

[3] Note that the concepts and patterns proposed are not meant to replace existing e-health concepts and patterns, such as the existing clinical terminologies or standard business process definitions but serve as a common reference point for human understanding and downstream enterprise modelling.

1.2 New Features in Version 2.0

The IF 2.0 provides a number of updates to the IF 1.0, with a particular emphasis on highlighting its foundational role in *implementing* interoperability solutions, including:

- The *use of the interoperability concepts and patterns* in harmonising enterprise modelling and enterprise architecture activities within Australian e-health;
- The application of several *interoperability guidelines* to facilitate interoperability design and analysis;
- The definition of appropriate *governance mechanisms and organisational practices* in support of interoperability readiness, such as certification processes, enterprise architecture program and an interoperability maturity program.

The IF2.0 reflects an increased level of maturity about interoperability, gained from discussions with key stakeholders within Australian e-health and through the further development of interoperability ideas. The aim is to continue providing impetus towards better national e-health interoperability. This is to be achieved through the transition from an initial state of shared understanding achieved since the publishing of the IF1.0 towards a broader focus of this version, including the pragmatics of implementing and adopting interoperability principles and practices in e-health projects.

This version provides a number of:

- *refinements*
- *extensions* and
- new *guidelines*

to those presented in the IF1.0 [IF1.0]

1.2.1 Refinements

The major *refinements* are grouped as follows:

- Clearer definition of the concept of interoperability than what was in the IF1.0;
- Interoperability modelling concepts:
  - Several updates to the existing category of interoperability languages, in terms of the respective organisational, information and technical concepts;
  - A minimal number of additions to this language category needed to provide better expressiveness for enterprise architecture purposes;
- Enterprise architecture framework:
  - Providing the rationale for adopting The Open Group Architecture Framework (TOGAF)[TOGAF] to guide architecture developments for national e-health infrastructure with which NEHTA is tasked;
  - Positioning of the interoperability languages as the modelling concepts for the enterprise architecture for national e-health infrastructure.

1.2.2 Extensions

The major *extensions* are grouped as follows:

- Interoperability patterns

  - a number of new categories of interoperability patterns were identified across the organisational, information and technical perspective;
  - the individual patterns within pattern categories are described using a proposed pattern form and where possible, examples are provided showing links to other interoperability patterns.
- Interoperability goals
  - these were developed for the purpose of interoperability maturity modelling, but can have a broader applicability, providing a detailed framework for interoperability analysis and design.
- Conformance, Compliance and Accreditation framework
  - a new framework was developed to describing key roles and their responsibilities in the certification space
- Interoperability Maturity Model
  - A framework based on the Capability Maturity Model Integration [CMMI], allowing e-health organisations to assess their existing interoperability parameters and define their interoperability improvements.

1.2.3 Interoperability guidelines

The interoperability guidelines consist of the following:

- Interoperability analysis and design guidelines describing
  - How to express interoperability in terms of constituent interoperability characteristics and treat them as interoperability goals to be achieved;
  - How to use interoperability concepts and patterns to realise the interoperability goals;
- Certification guidelines
  - Describing steps to be taken and options available for conformance, compliance and accreditation processes.
- Interoperability assessment method
  - Providing guidelines for the use of the Interoperability Maturity Model (IMM) and consisting of:
    - a set of steps to be applied when assessing current interoperability parameters of e-health projects;
    - a set of steps for defining interoperability maturity programs for e-health projects.
- Interoperability roadmap
  - Positioning all interoperability tools and guidelines in relation to each other, serving as a roadmap for their use

1.3 Intended Audience

This document is intended for:

- CIOs and CTOs within jurisdictions and e-health organisations;
- Strategic planners, clinical informatics experts, business analysts and interoperability architects, enterprise architects and solution architects.

Note that although this document involves a significant level of technical content it is structured in a way that can be used by different audiences above, as per instructions given in section 1.5.

1.4 Structure of the document

This document follows the structure of the earlier version of Interoperability Framework [IF1.0] to provide easy reading for those already familiar with the IF1.0.

The document consists of the following parts:

1. Interoperability Framework description – outlining key features of the NEHTA IF, as a family of languages facilitating shared understanding of interoperability. This is presented in Chapters 2, 3, 4 and 5.
2. Introduction to Compliance, Conformance and Accreditation issues – providing the basis for understanding a set of certification capabilities and developing a certification program for Australian e-health. This is presented in Chapter 6.
3. Introduction to Enterprise Architecture for National e-Health infrastructure – setting the scene and direction for the NEHTA Enterprise Architecture activity[4]. This is presented in Chapter 7[5].
4. Interoperability guidelines – describing several useful approaches of relevance for analysing, defining and measuring interoperability. This is presented in Chapter 8.
5. Introduction to Interoperability Maturity Model – capturing key ideas from the NEHTA Interoperability Maturity Model (IMM) [IMM]. This is presented in Chapter 9.
6. Standards Catalogue outline. This is presented in Chapter 10.
7. Next steps, outlining future IF developments recognised at the time of writing, presented in Chapter 11.

1.5 How to use this document

This Interoperability Framework can be used as a starting reference point for both existing and new e-health stakeholders in Australia. This includes:

- Strategic planners concerned with the enabling role of technology in the delivery of healthcare services; they should read Chapters 1, 2, 6 and 9 of this document;
- Clinical informatics experts concerned with the meaning of information and information models representing various clinical artefacts and ontologies; they should read Chapters 1, 2, 3, 4, 6 and 9;
- Business analysts concerned with capturing business and functional requirements from domain experts and translating them into a form compatible with the expression of enterprise architectures; they should read Chapters 2, 3 and 7;
- Enterprise architects and solution architects concerned with developing enterprise architectures or specific solution architectures; they should read all Chapters of this document.

1.6 Interoperability Roadmap

Figure 1 depicts key documents produced by NEHTA on its path from development towards implementation stages of interoperability solutions.

[4] Further details about Enterprise Architecture will be published in a separate document.

[5] Note that this section includes key points on the IF methodology (which was a separate section in the IF1.0).

This evolutionary path of the Interoperability Framework (IF) specifications, beginning with the version IF1.0, reflects increasing maturity in the understanding, development and implementation of interoperability solutions.

For example, this version, the IF2.0, provides a number of extensions and refinements of the modelling concepts from the IF1.0 as well as a number of new guidelines and methodologies that support implementation of interoperability solutions. These new elements in the IF2.0 are influenced by the specifications from other interoperability documents, i.e. Enterprise Architecture (EA), Conformance Compliance and Accreditation (CCA) and Interoperability Maturity Model (IMM)[6] produced after publication of the IF1.0. Note that the development of these specifications was influenced by the principles and modelling elements adopted in the IF1.0, as shown in the figure.

The figure also depicts the role of case studies as a feedback mechanism for collecting new interoperability requirements and approaches.

Finally, it is anticipated that subsequent versions of the Interoperability Framework will be influenced by new solutions from the EA, CCA and IMM spaces, and possibly by other interoperability factors and developments.

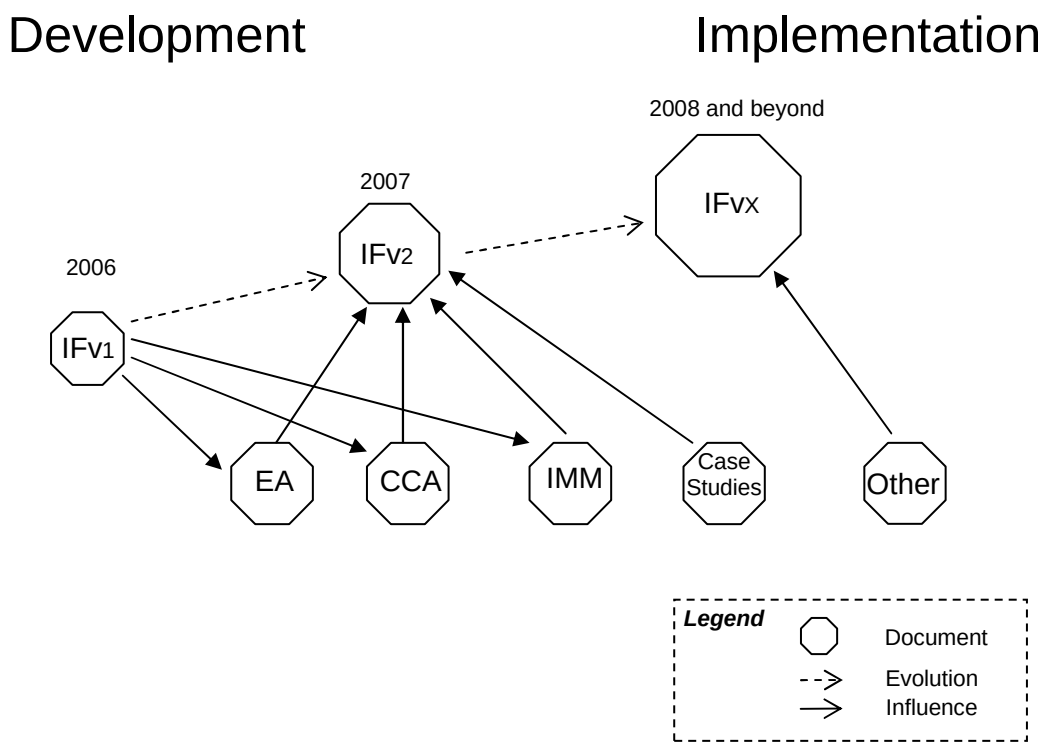

Figure 1: Interoperability Roadmap

[6] At present, only the Interoperability Maturity Model has been made publicly available [IMM].

2 Interoperability Framework

The health sector in Australia is a diverse community consisting of individual health provider organisations and jurisdictions delivering care through a range of channels and with varied technical and management capabilities. The various facets of this community need to be taken into account when designing and deploying ICT systems in support of interoperable healthcare delivery.

2.1 Interoperability: Australian e-health context

In this context, interoperability needs to be understood in broader terms than the traditional technical notion of ensuring connectivity and integration between Information technology (IT) systems and the adoption of appropriate technical standards. Interoperability in e-health also needs to address policy and organisational issues that reflect the main purpose of e-health, namely, providing better, safer and more efficient healthcare delivery.

This emphasis on organisational issues is supported by a recent IEEE (Institute of Electrical and Electronics Engineers) e-health initiative emphasising the fact that 'interoperability refers not so much to machines working together but human beings understanding each other' [IEEE]. On the path to achieving an electronically interoperable environment, the initial requirement is realising a shared understanding in delivering e-health results [NEHTAIF1.8], including a shared understanding of organisational, information and technical issues. This is directly reflected in the NEHTA Interoperability Framework.

A national approach to interoperability is vital to the Australian e-health agenda. This is because it contributes to enhanced healthcare delivery by facilitating realisation of continuity of care and continuum of care[7] principles and better decision making while delivering anticipated cost savings [BCG]. These cost savings can be achieved through adoption of new technologies, more effective business practices, governance approaches and acquisition strategies. Interoperability also prepares for the unforseen consequences resulting from the replacement and renewal of health systems or from changes in business expectation.

This section begins with a definition of interoperability that reflects that broader context. It then explains the role of the Interoperability Framework as a vehicle for promoting shared understanding about e-health related issues in Australia. This is followed by the description of the relationship between the IF and enterprise architecture topics and the support in treating interoperability as a continual state of readiness.

2.2 Defining Interoperability

It is recognised that 'coming to terms' with interoperability in e-health is a challenging task because it involves two communities of practice known for their use of complex and difficult languages: medicine and computer science [HL7 Interop].

[7] Continuity of care refers to the exchange of information and delivery of healthcare services in the context of a single healthcare episode while continuum of care refers to seamless transitions from one type of healthcare setting to another, e.g. from prevention via detection and then management to rehabilitation.

NEHTA is attempting to address the needs of both of these communities by defining interoperability as:

> *The continual ability of an organisation (or a system) to use or offer business (or technical) services from or to another organisation (or system) and accordingly, exchange information (or data) with other organisations (or systems) to achieve a specified purpose in a given context.*

This definition suggests a need to consider organisational issues, semantics of information, constant readiness and the boundaries that define the context or domain of interoperability[8]. Again, this is in addition to the traditional interpretation of interoperability in terms of connectivity.

2.2.1 Interoperability Principles

The definition above can be used to emphasise several fundamental interoperability properties, namely:

- Multi-dimensional issue – not only a technical concern;
- Continual requirement – not only at a certain point in time;
- Cross-organisational issue – not only processes but also policies.

These properties have influenced the emergence of five key interoperability principles adopted in this Interoperability Framework:

1. Semantics principle – agreement on the meaning of languages to be used to communicate and/or model real world entities by each group of stakeholders (from technical, information and organisation perspectives);
2. Heterogeneity principle – information exchange and use in spite of various implementations;
3. Readiness principle - interoperability is a continual state of readiness;
4. Federation principle – collaboration in spite of organisational autonomy;
5. Domain principle – interaction boundaries determine interoperability problem.

The first principle requires a common agreement about interoperability concepts and approaches and often relies on the use of open standards.

The second principle requires focus on architecture, standards or other specifications, allowing for freedom in the choice of implementation options.

The third principle is about the state of readiness, in terms of being able to react to change and adopt technology, clinical solutions or regulatory changes.

The fourth principle is a recognition that each organisation or health jurisdiction will have their own clinical and administrative processes and policies, but the continuity of care and continuum of care clinical principles require collaboration in spite of these differences.

The fifth principle emphasises the fact that interoperability means different abilities in different contexts – local, organisational, national or even international domains.

In addition to these fundamental principles, each of the technical, information and organisational perspectives are characterised by additional sets of principles which will be described as part of these perspectives in subsequent sections.

[8] These domains are community, organisational and local domains as will be elaborated in section 8.4.

2.2.2 Interoperability Characteristics/Goals

The definition of interoperability implies the multi-faceted nature of interoperability in e-health. We refer to these different facets of interoperability as *interoperability characteristics.* Examples of such characteristics are reuse, evolution, standards adoption, explicit specification of business context, business services, separation of specification from implementation and so on.

An interoperability characteristic is thus one specific facet of interoperability that an organisation or a system needs to establish in order to effectively interoperate with other organisations or systems. The characteristics are used as a way of abstracting different interoperability facets. Section 8.1 provides a complete list of interoperability characteristics identified so far.

Interoperability characteristics, when accompanied with the corresponding measures, can be regarded as *interoperability goals* to be achieved to support the corresponding interoperability facet. This is of particular relevance for interoperability maturity approaches as will be discussed in Chapter 9.

2.2.3 Interoperability vs Integration

The NEHTA IF places importance on articulating the following distinction between interoperability and integration.

Interoperability is taken to mean a continual state of readiness to exchange meaningful data/information and participate in collaborative healthcare delivery. The key assumption here is that change is the only constant and thus, an approach needs to be developed that prepares all the stakeholders for previously unforseen consequences of change. These consequences may be a result of replacement and renewal of health systems or changes in legislative or social environments.

So, when developing future solutions based upon current problem analysis (shown as green 'projected' circles into a 'projected future delivery' state in Figure 2), one needs to recognise that the final delivery may not meet changing requirements. The new solution requirements (depicted as red circles in Figure 2) may not match the projected solution deliveries. This is because of the change that is likely to occur over time, be it due to a technological, business or policy-based issue. In other words, the 'projected future delivery' space is likely to differ from the 'required future solution' space (shown as a box in Figure 2).

Integration on the other hand is seen as a slice through an interoperability time line, describing a moment in time where systems are interconnected to provide solution delivery.

In summary, interoperability is a necessary precondition to ensure longevity of integration in a changing IT and, more importantly, business environment. Interoperability creates a space for integration solutions that works *with* change rather than against change.

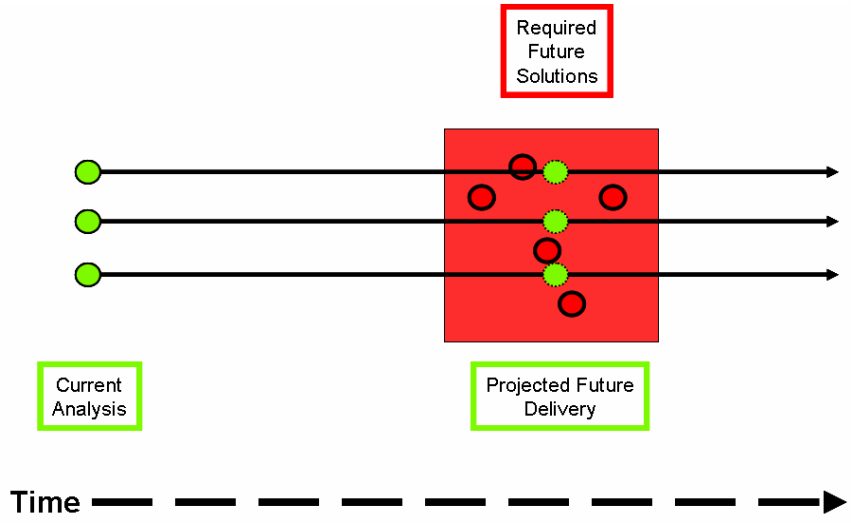

Figure 2: The essence of interoperability—allowing for a changing future

2.3 Interoperability Concepts and Patterns

The NEHTA IF aims to develop a shared understanding of interoperability issues, to promote compatibility and interconnectivity in Australian e-health. This shared understanding is based on two key features (see Figure 3):

- *interoperability concepts* and the corresponding *interoperability language* for expressing them; 'language' here refers to shared terminology defining the concepts needed to facilitate communication and shared understanding of the various dimensions of e-health. The language must be defined with sufficient precision to be used for downstream architecture specification and modelling activities;
- a set of *interoperability patterns,* introduced as a mechanism for capturing frequently occurring issues and observations in e-health and reusing them in different contexts (e.g. by different e-health projects).

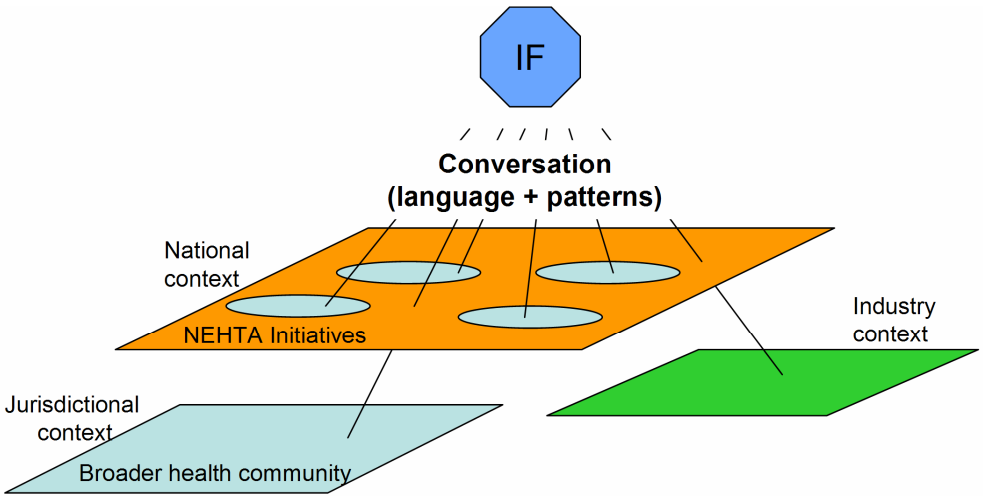

Figure 3: Facilitating a shared understanding through the IF

Figure 3 depicts symbolically how the interoperability language and patterns are applied. The language and patterns provide the common conceptual and semantic underpinnings harmonising conversation within NEHTA first, i.e. among NEHTA initiatives (shown as blue ovals in the upper orange plane). The language and patterns are then propagated into the broader jurisdictional

context, ensuring a shared understanding of organisational, information and technical interoperability concepts, as well as interoperability patterns, among both business and technical stakeholders in the broader Australian health community[9]. This figure also shows a need for a broader scope of interoperability such as interoperability within an industry context (examples include supply-chain stakeholders as well as government sectors such as emergency services and non-government organisations).

While the interoperability languages provide a foundation for shared understanding, the interoperability patterns add further value to this understanding by capturing common knowledge about the issues that occur when building e-health systems. For example, they enable the capture of common issues encountered by NEHTA and jurisdictional projects, enabling other projects to recognise similar challenges and leverage recognised interoperability approaches and thus reduce duplication of interoperability efforts.

2.3.1 Interoperability Concepts

Interoperability concepts describe the common semantics of real-world entities from business, clinical, and IT systems perspectives while leveraging relevant open standards. These concepts are described in detail in sections 3.3, 4.3 and 5.3 and this section provides background information about the open standard that were selected as their foundation.

The concepts selected are based on two requirements. Firstly, they needed to form a minimal set of core concepts needed for business, clinical or IT systems perspectives. Secondly, they needed to be expressed with a sufficient precision to support downstream enterprise architecture and enterprise modelling activities. These two requirements are met by leveraging of a system-theoretic framework for describing architectures of open distributed systems. This framework is a family of ISO standards known as the Reference Model for Open Distributed Processing (RM-ODP) [ODP-RM].

The RM-ODP standards recommend viewing any complex open distributed system from different viewpoints, enabling separation of concerns associated with different stakeholders involved. Each viewpoint includes the definition of a number of language concepts and structuring rules for describing relationships between these concepts.

The RM-ODP has influenced several other industry standards, most notably the Unified Modelling Language (UML) [UML] and Model-Driven-Architecture (MDA) [MDA] in the Object Management Group (OMG). In particular, the latest standardisation efforts on UML profile for ODP [UML ODP], being finalised by ISO, will provide a strong foundation for model-driven engineering of e-health systems, owing to the increasing availability of tools supporting model-driven development. This has particular significance when considering interoperability implementation activities, including requirements capture, enterprise modelling and enterprise architecture.

In addition the RM-ODP standards have been used in the health domain, e.g. in the ISO Health Informatics Profiling Framework standard [HIPF] and most recently within the Health Informatics Service Architecture [HISA].

The interoperability concept definitions and their relationships constitute an interoperability language, or more precisely a family of interoperability languages to reflect the structuring of the IF, as explained in section 2.4.

Note that this version, the IF2.0, incorporates several refinements and extensions of the concepts from the IF1.0.

[9] It is important to note that different administrative boundaries determine different interoperability requirements and this will be elaborated in section 8.4.

In addition to the interoperability concepts, which are based on sound semantic foundations, the IF provides allowance for additional interoperability vocabulary, in terms of interoperability patterns. The idea behind interoperability patterns is that of pragmatics, i.e. to support description of typical situations in e-health and their interoperability challenges and solutions. This is done over time so that the pattern vocabulary grows and evolves as a result of many contributions of e-health practitioners. Thus interoperability patterns describe frequently occurring e-health situations (e.g. referral processes), in terms of specific relationships between interoperability concepts.

2.3.2 Interoperability Patterns

2.3.2.1 Background

The interest in patterns in IT has surfaced as a result of work by Christopher Alexander in the area of architecture [Alexander] and has resulted in the adoption of his ideas in the area of software development [GOF].

In general a pattern describes a recurring problem in a particular environment and the core of the solution of that problem that can be reused in different situations. Patterns are identified through experience and they thus document proven approaches to solving certain problems. In some cases, there may be justification for promoting patterns into first-class modelling concepts, provided their frequent use and well-defined semantics justify it.

Patterns include structural or behavioural relationships between system parts and various constraints that may apply to these relationships. They are identified over time and they are typically added in a piecemeal manner to form a catalogue of solutions available for reuse.

2.3.2.2 NEHTA approach

The NEHTA IF adopts a similar, pattern-based approach in identifying frequently recurring situations pertinent to interoperability in e-health. These interoperability patterns can be regarded as a specific way of supporting interoperability goals.

One motivation for adopting patterns is first in *identifying issues* that are recognised as possible hindrances to interoperability and thus serving as an interoperability 'check-list' for e-health projects. A broad grouping of related issues, e.g. governance issues, form what is called in this document a *pattern category*.

The second motivation for adopting a patterns approach was driven by the value that can be found in *reusing common approaches* to addressing these issues to ensure that valuable principles and interoperability approaches have been preserved and applied across various contexts.

Note that the IF1.0 has identified several pattern categories but without nominating specific patterns therein. Essentially, they served as placeholders for a number of specific patterns that were identified since the publication of the IF1.0, and which are presented in this document.

Interoperability patterns are described using the interoperability concepts. The purpose of patterns is to describe the ways that concepts are related to produce some effect i.e. capturing core solutions to frequently occurring problems. The core solutions can then be parameterised, to reflect context of the specific problem in question.

2.3.2.3 Presentation style

In this document (as also in the IF1.0), interoperability patterns are classified first in terms of the *interoperability perspectives* in which they can be applied (viz organisational, information and technical – see section 2.4).

Within each of the perspectives, a number of pattern *categories* are identified.

This version first presents those categories that are structured in terms of the constituent interoperability patterns, i.e. those that can be directly reused as common solution approaches, thus reflecting the second motivation above. In the case of such structured categories, it was possible to identify specific patterns and these are described using an *interoperability pattern form* developed for the purpose of the IF. These pattern categories thus provide more guidance in terms of the reuse of common approaches. For example, several policy patterns are identified within the category of legislative, regulatory and enterprise policies.

These type of categories are then followed by the description of those pattern categories that have only the purpose of identifying common issues (and thus reflect the first motivation above), as was the case with the original categories presented in the IF1.0. These categories are to be considered as placeholders for new interoperability patterns anticipated to be captured in future.

One pattern can be related to many other patterns and one pattern can belong to several pattern categories.

The interoperability pattern form developed has the following structure:

- Pattern name
- Description, including the context and purpose of the pattern
- Solution
- Examples
- Pattern category
- Related patterns (where applicable).

In summary, in the IF1.0, interoperability patterns were introduced in terms of broad grouping of different interoperability situations and thus the primary focus was on identifying broad categories of patterns. This version begins with the introduction of interoperability patterns in a form that is more suitable for cataloguing, through the adoption of the interoperability pattern form above. In addition, there are a number of new patterns and pattern categories that were identified, taking into account several case studies that were undertaken since the publication of the IF1.0.

2.4 Structure of the IF

The IF consists of three separate but related interoperability perspectives (see Figure 4):

- The organisational perspective;
- The information perspective;
- The technical perspective.

The organisational perspective is concerned with the understanding of the legislative, regulatory, healthcare and enterprise environment in which IT systems need to be deployed to enable improved healthcare delivery. This requires agreement on key organisational concepts such as roles, policies and processes as well as capture of relevant organisational patterns such as legislative compliance, governance, and change management.

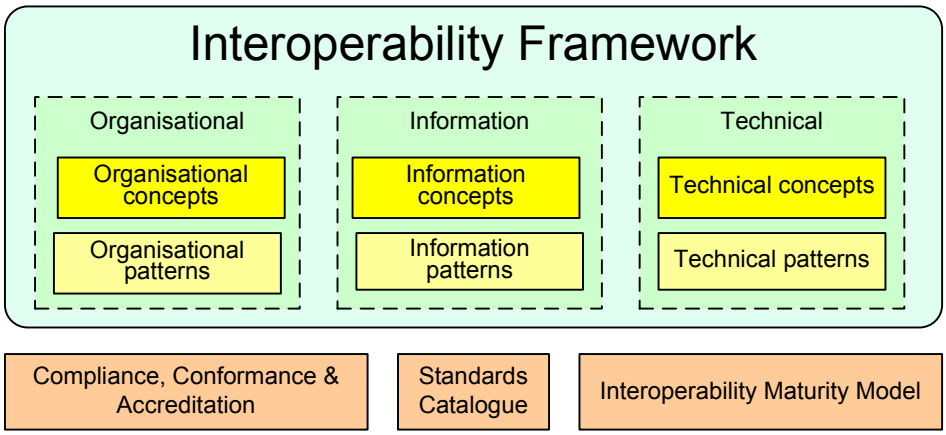

Figure 4: The Interoperability Framework and related components

The information perspective is concerned with how clinical, administrative or statistical information can be represented and interpreted. Information is taken to be 'any kind of knowledge that is exchangeable amongst users, about things, facts, concepts and so on, in a Universe of Discourse' [ISO/IEC 10746-2]. This requires agreement on a core set of information concepts, such as information components and relationships between components, as well as capture of relevant information patterns such as information rights, information quality and scope of application.

The technical perspective is concerned with the understanding of technical functionality for delivering e-health systems. This requires agreement on a core set of technical concepts, such as technical service, interface, technical components and interactions, as well as capture of relevant technical patterns such as styles of component interactions and technical architecture styles.

These perspectives are different viewpoints on the one system. A system can be anything of interest, either as a whole, or as composed of its parts. Examples are

- particular e-health applications such as a health provider index, e-prescribing or clinical terminology service,
- an e-health 'domain' such as pathology or radiology,
- an e-health entity such as a General Practitioner's practice,
- a hospital,
- or even the whole e-health system in a region or country.

It is important to note that depending on the system in question, the individual perspectives will be populated to varying degrees of detail as some put a greater emphasis on different delivery aspects. For example, an information model is information intensive while a policy framework is organisational intensive but it may have some aspect of its definition in information or technical perspectives.

The IF is structured in this way to support the expression of different concerns of the stakeholders in e-health while recognising the inherent complexity of e-health systems. Each of the three IF perspectives, has its own set of interoperability language concepts and interoperability patterns. In addition, there are a multitude of relationships and dependencies between the language concepts and patterns across the perspectives (e.g. an organisational concept relates to an information concept). This reflects the fact that the three IF perspectives should always refer to one system and they should be considered together when specifying a system.

This approach to the IF was chosen to address the complexity of e-health systems, resulting from the heterogeneous, multi-jurisdictional, multi-domain, cross-boundary, and (increasingly demanded) consumer-centric characteristics of the Australian e-health environment. So, this environment

requires addressing not only information and technical interoperability (that has seen much of the effort in the past), but also *organisational* interoperability. The former deals with the interoperation of information and technical solutions, such as in traditional middleware approaches, while the latter deals with the business context.

This breakdown is in line with several national and international interoperability frameworks [AGTIF], [eGIF], [EIF], [EPAN].

Figure 4 also shows some related components such as the standards catalogue, the compliance, conformance and accreditation framework (CCA) and interoperability maturity model.

2.5 IF and Enterprise Architectures

The NEHTA IF recognises the co-existence of many jurisdictional e-health efforts in Australia and is not intended to replace or mandate specific enterprise architecture (EA) approaches. Rather, the aim is to provide an overarching interoperability framework that can accommodate existing systems and developments while ensuring alignment and harmonisation of future e-health architecture and systems as appropriate (see Figure 5). Examples of such future e-health efforts are individual healthcare identifiers and shared electronic health record systems. This section lists some key commonalities and distinctions between the IF and typical EA themes.

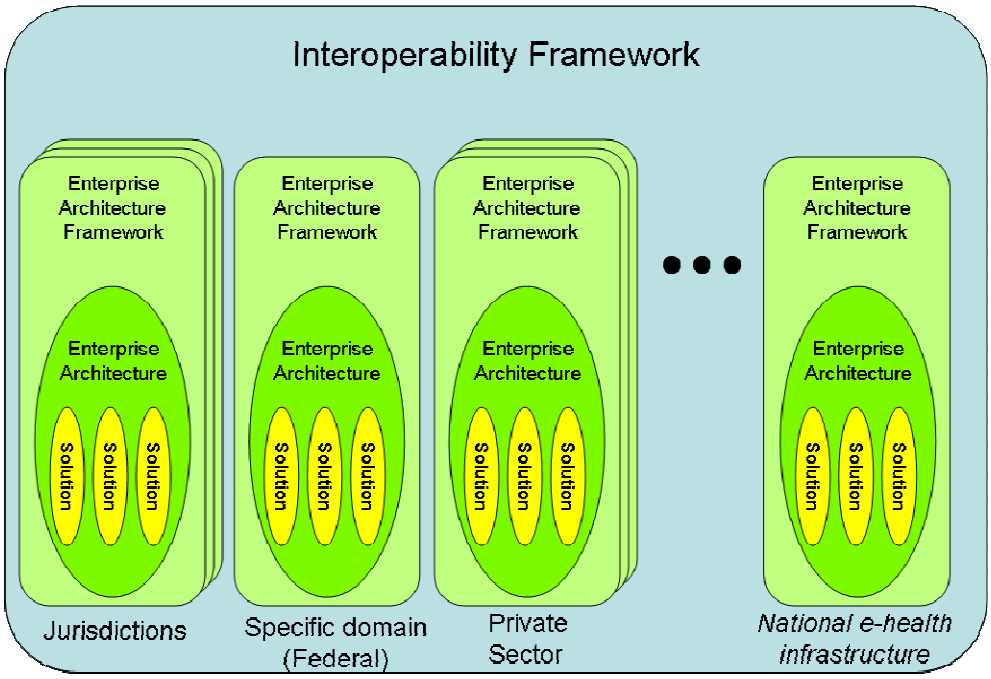

Figure 5: IF and Enterprise Architectures

The IF can be seen as a coordinating framework for various jurisdictional Enterprise Architecture Framework (EAF) developments, incorporating a common philosophy – but one that only defines a small set of interoperability concepts and interoperability patterns needed to ensure architectural alignment within NEHTA and more broadly in the e-health community.

The following correspondences can be made between the IF and commonly used EAFs:

- The organisational perspective relates to an EAF's business architecture;
- The informational perspective relates to an EAF's information architecture; and
- The technical perspective relates to an EAF's application and technology architectures.

2.5.1 Distinguishing features

There are several distinguishing characteristics of the IF when compared to many EAF approaches.

First, the IF provides a more complete set of business concepts than Enterprise Architecture Frameworks. In particular, the e-health requirements outlined in section 2.1 require placing a special emphasis on the concept of business, legal and health-related *policies*. Policies are important to support controlled access to and use of sensitive medical information in support of continuity of care requirements. This in turn requires a generic and precise framework for describing how policies relate to business processes, business services, business roles and applications involved in delivering e-health. Such a framework should also recognise and support the implications of possibly multiple sources of policy origin, such as policy conflicts and their need for resolution.

Second, the IF, similar to the ODP standards, adopts a specification style that gives an emphasis to *action* (rather than state). This is motivated by a need to support a well-defined conformance model allowing observation (i.e. testing) of systems against specification – because actions are observable[10].

The concept of action is defined as 'something which happens', and this concept applies to the organisational and technical perspectives. In fact, the concept of action is a fundamental concept for describing many behavioural expressions in either of these perspectives. Examples in the organisational perspective are actions performed by clinicians or IT systems, possibly as a part of more complex business processes and privacy policy expressions stating constraint on who is allowed to perform access to sensitive health information. Examples in the technical perspective are interactions between software components in a clinical information system or exchange of messages in a supply chain system.

The third feature of the IF is a distinction between *interoperability patterns* identified in the IF and the *patterns* of relevance for downstream architecture developments, referred to as solution patterns. The IF interoperability patterns specifically reflect the e-health environment in Australia and are captured to flag the existence of commonly occurring structures and arrangements that, if not addressed, could provide potential hindrance to interoperability.

The interoperability patterns can in turn serve as a framing mechanism for a number of solution patterns. While interoperability patterns are identified with an e-health context in mind, defining certain relationship between interoperability concepts, the solution patterns have a more generic ICT character describing certain relations between ICT components, e.g. structural relationship between classes or communications between software components.

Solution patterns can be further categorized into architectural, design and test patterns. For example, they can define some common types of business processes in health such as referrals and apply them to various contexts, e.g. GP to hospital, GP to specialist or even GP to pathologist orders. The purpose of solution patterns is to exploit past knowledge of solution approaches to arrive at solutions faster, using proven techniques.

New patterns, either interoperability or solution patterns, are discovered over time as certain recurring core solutions are observed to be used to solve specific problems. They can then be identified as potential candidates to address similar problems in future and documented as appropriate. In this respect, patterns can be regarded as an asset that can be used to facilitate the development and production of models, products and systems.

---

[10] One can argue that states are observable through probing the state – but probing itself is an action [Linington].

Therefore, it is the IF concepts and patterns, which when propagated through various EAFs, enhance the common understanding and architectural alignment across various e-health architectures. Each jurisdiction is likely to have their own EAF, which is the basis for developing many compliant architectures such as specific solution architectures.

Finally, the IF introduces an overarching methodology (presented in section 7.2) supporting a link between business requirements and architectural specifications with a certification process enabled through compliance and conformance. EAFs are also associated with methodologies that prescribe the steps required to fulfil the requirements of the EAF. These are usually presented separately from the EAF itself. The relationship between the IF methodology and such EAF methodologies is described in section 7.1.

2.5.2 IF compliant Enterprise Architecture: NEHTA approach

In order to ensure that various architecture developments within NEHTA are compliant with the IF, NEHTA has adopted an EAF that can effectively accommodate the IF concepts and patterns, namely The Open Group Architecture Framework (TOGAF), version 8.1[11] [TOGAF8.1].

The use of TOGAF:

- Allows the propagation of the IF modelling language concepts into the constituent business, information systems and technology architectures, according to the correspondences indicated at the beginning of this section; the NEHTA customisation of TOGAF prescribes the use of these concepts for defining specific architectures;
- Supports the propagation of interoperability patterns into the TOGAF enterprise continuum;
- Fosters the treatment of architecture developments as an iterative and incremental process, through the use of the TOGAF's Architecture Development Methodology (ADM); this methodology can be seen as refinement of the IF methodology.

It is worth noting that TOGAF is used to define a technical strategy and structure for ICT components within the NEHTA work program that contribute to the national e-health infrastructure. Further details are provided in section 7.3.

2.6 Approach to sustainability and evolution

The establishment of an overarching and long lasting interoperability framework for e-health in Australia, initially promoted and adopted by NEHTA, and subsequently by the broader e-health sector, will be achieved through:

- *Encouraging discussions* and setting forth an agreed way of describing interoperability;
- *Documenting* the approaches, policies, patterns, information, technologies and standards, that are shared across the health sector; this function is partly addressed through the NEHTA *standards catalogue*, which will be a living artefact that contains a list of standards currently endorsed by NEHTA, whether defined by NEHTA or other Standards Development Organisations (SDOs);
- Establishing an *IF methodology* aiming at economically sustainable outcomes and in the interest of public health. This methodology facilitates enforcement of interoperability principles, in particular

[11] It is anticipated that the forthcoming version of TOGAF (version 9.0), when adopted, will be used in subsequent architecture developments by NEHTA.

through the separation of requirements, specification and implementation, and certification of implementations. This in turn allows for a competitive approach to the delivery of interoperable e-health systems and serves as an insurance policy against changes in technologies and business context;

- Adopting a clear distinction between *compliance* and *conformance,* as highlighted in the ISO/IEC RM-ODP standard [ODP-RM], as part of the IF methodology:
  - Compliance is about checking the extent to which specifications rely on standards as an interoperability mechanism; and
  - Conformance is about checking whether solutions and products satisfy specifications which they claim to implement.
- A *disciplined approach* in applying key phases of the IF methodology (see section 7.2 for further details), i.e.:
  - Capture of the *requirements* for e-health systems, from all three IF perspectives, with a particular emphasis on using organisational concepts and patterns;
  - Development of a consistent set of *specifications* based on requirements; these in turn will facilitate compatible solutions for the delivery of an interoperable, whole-of-health environment; again, this will be done from all three IF perspectives;
  - Definition of a clear set of *conformance points* in specifications which can be used as a basis for checking the extent to which products and solutions satisfy the NEHTA specifications; these can serve as a basis for subsequent certification of these products; and
  - A *continual value assessment* of the benefits realised. This assessment is needed to monitor the investment and identify points of improvement that may be needed due to the restructured business processes or new technologies.
- The adoption of *interoperability maturity modelling* to ensure continual improvements of organisations' abilities to interoperate;
- The *proactive engagement* of jurisdictions and other stakeholders to ensure cross-fertilisation and alignment between NEHTA efforts and other developments in Australian e-health.

2.7 Summary

The IF delivers a single source of NEHTA guidance for all of the healthcare community and should be used as the basis for long-term business and systems alignment [NEHTAIF1.8].

The IF can provide valuable contributions towards aligning various enterprise and solution architecture activities.

An important part of the IF is the iterative, incremental and evolutionary methodology which distinguishes requirements, specification, conformance and value assessment phases.

The ultimate goal is to facilitate development and continuous evolution of e-health systems to ensure that in the care of patients, all required information for medical decisions and care is correct and available in a timely manner to health professionals.

The following three chapters describe the perspectives of the IF in more detail.

3 Organisational perspective

The organisational perspective of the IF (OIF) addresses the business context as well as legal and policy issues of relevance for understanding, specifying and deploying e-health systems. The OIF allows for the description of business processes, business policies and organisational structures, covering the scope of intra-organisational, inter-organisational and cross-jurisdictional interactions. This also supports the description of both the strategic and operational governance aspects of various corporate and technology structures.

3.1 Background

The organisational perspective is becoming more important in response to the increasingly broadening scope of e-health applications that involve multiple providers and more direct participation of consumers.

NEHTA recognises the importance of organisational interoperability issues and is at the forefront of a number of international e-health initiatives, by placing a special emphasis on this context. Examples of related initiatives are the CEN251 work on the Health Informatics Service Architecture [HISA] and the recent attempts by the HL7 EHR Interoperability Work Group to scope and define interoperability for Health Care [HL7 Interop].

The NEHTA OIF meets most of the requirements stated in these international standardisation efforts through an expressive language for describing concepts of relevance for the organisational perspective such as collaborative communities, business processes, business services and roles. In addition, the OIF addresses further challenges by providing a strong emphasis on defining and relating policies to business processes, roles and services. These are important issues in view of the cross-organisational collaborations and cross-jurisdictional concerns, currently beyond the scope of HISA and HL7 interoperability efforts.

The OIF is based on the RM-ODP Enterprise Language (ODP-EL) standard from the family of RM-ODP standards. The ODP-EL was chosen because it:

- Provides a small number of generic organisational concepts for describing structural, behavioural and policy concepts. While close to everyday business jargon (e.g. the concepts of business service, business process, role, party and so on), these terms have a precise meaning, grounded in a number of theoretical and modelling techniques;
- Can be further extended to reflect specific needs of the e-health domain such as policy and privacy concept frameworks, specific health-care roles and business processes, as well as clinical concepts.

This version of the IF:

- Begins by identifying key organisational interoperability principles;
- Defines several new organisational concepts, namely: actor, artefact, resource, location (in space and in time), distribution and business function;
- Refines the existing concept of business process with several new concepts, i.e. business function, input and output artefacts to process, and sub-process;
- Provides several new categories of patterns, namely: policy conflict resolutions, standard business processes, corporate memory, monitoring and audit;

- Describes existing patterns using the pattern form introduced in section 2.3.2.

3.2 Organisational interoperability principles

The organisational interoperability principles refine and extend the general interoperability principles from section 2.2.1. These organisational principles are stated as follows:

- Provide a well-defined organisational context for interaction;
- Make explicit statements of business objective and value contributed by IT;
- Separate basic interactions from the related policy constraints;
- Ensure a high level of protection for health information.

The first principle states that a boundary for interaction between organisations or systems need to be well understood because the policies that apply within and across boundaries are different and impact interoperability. The implication of this principle is a need for explicit expression of organisational boundaries.

The second principle emphasises the importance of well-articulated business objectives of an organisation or community and how the IT systems implemented support this objective. The implication of this principle is that there needs to be a way of defining value that IT brings to the organisation or community.

The third principles takes into account the fact that many organisational changes come from changes in policies which in turn often come from changes in strategy. On the other hand, the fundamental (or basic) interactions represent inherent behaviour and they are less subject to change. The implication of this principle is to that policy should not be embedded into description of business processes.

This fourth principle is motivated by the sensitive nature of health information. Note that according to the Commonwealth Privacy Act, *health information* is defined as [Priv]:

- information or an opinion about:
  - the health or disability (at any time) of an individual; or
  - an individual's expressed wishes about the future provision of health services to him or her; or
  - a health service provided, or to be provided, to an individual.
- other personal information collected to provide, or in providing, a health service; or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

The implication of this principle is a need for defining and enforcing policies that cover access to, use and exchange of healthcare information.

3.3 Core Concepts

The key OIF concept is that of community, providing the overarching context for expressing business structures, business processes and business policies in a way which is independent of the specific entities that participate in the

community. This ensures longevity of specifications and the ability for many instantiations of the structural and behavioural aspects of the community.

Although inspired by the everyday use of the word 'community', the OIF community has a precise meaning developed to support the capture of requirements and development of unambiguous specifications.

In the following subsections, the concept of entity is first defined, followed by the description of a number of organisational concepts related to the community.

3.3.1 Entity

An *entity* is any abstract or concrete thing in a Universe of Discourse. An entity has its own identity and own life cycle. Note that this life cycle is independent of life cycles of communities in which it may participate (see the next section for the definition of community concept).

Recall the concept of action introduced in section 2.5.1. With respect to a given action, an entity can be related to the action in one of the following ways:

- as an *actor* with respect to the action, if the entity participates in the action; these can be humans, organisations or IT systems that generate alerts or notifications;
- as an *artefact* with respect to the action, if it is referenced (mentioned) in the action; an artefact can be used by some other entity, e.g. the use of a specification document by an architect, or it can be produced by some entity, e.g a design document as an output of a design process or reports generated through a testing and certification process (see section 6.3.3 on the specification community);
- as a *resource* with respect to that action, if it is essential for the performance of that action and may require allocation or may become available; a resource may be a special kind of an actor, e.g. a nurse in a hospital, an enterprise architect within a jurisdiction's ICT department or a special kind of an artefact, e.g. a bed in an emergency department.

Any given entity may relate to different actions in more than one of the ways above, e.g. CT scanner can be an actor when the action is 'CT scan' and a resource when the action is 'schedule CT scan for patient X'.

Typically, an entity can join a community for the purpose of satisfying its objectives which can be achieved from the participation in the community.

3.3.2 Community

Community is defined as a configuration of entities (e.g. individuals, organisations, information systems, or various combination of these), able to interact and established to meet some objective.

Communities can be related to each other in hierarchical or peer-to-peer arrangements.

Community is specified in terms of *community roles* and a community *contract.*

3.3.3 Community role

The *role* in a community specifies part of community's structure and behaviour and can be filled by various entities, including the entities that represent other communities. An entity can be assigned to a role in the community subject to the role-filling (or assignment) policies.

An entity can fill a role in more than one community at a time.

Roles partition community structure and behaviour to reflect specific organisational arrangements. The roles in the community are defined by some community authority.

Figure 6 depicts an actor (e.g. Dr Mary Brown) filling a role in a community (e.g. a hospital) or another community filling another role (e.g. a pharmacy within the hospital). The dashed circles in the diagram depict roles in the community.

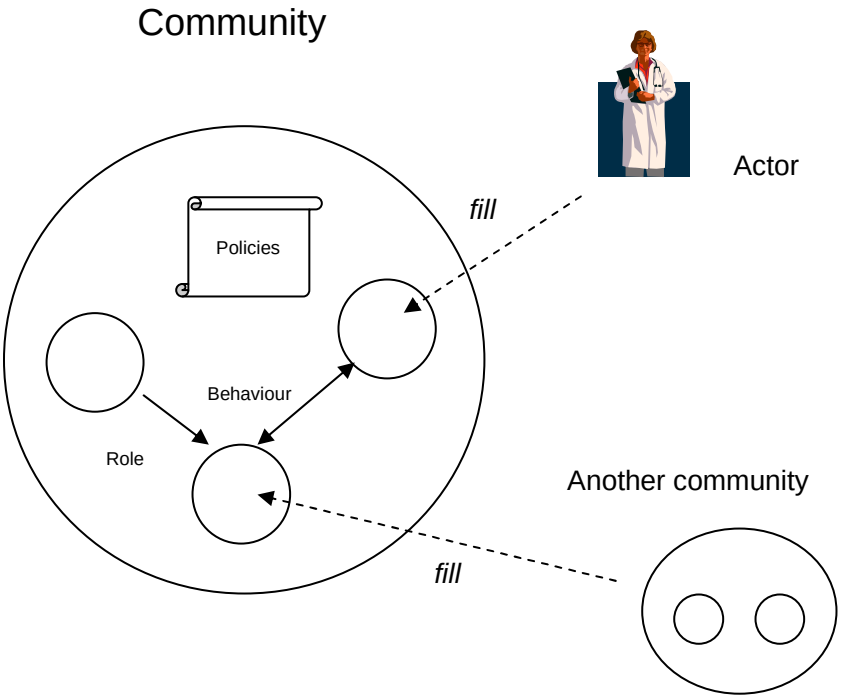

Figure 6: Entity and Community

3.3.4 Community contract

A community *contract* (or community specification) specifies the agreement that must exist among the entities filling the community roles to work together in order to meet the community objective.

A community contract:

- States the objective for which the community exists;
- Governs the structure, behaviour and policies of the community, in terms of the roles in the community and their relationships; the behaviour can be in terms of structured business processes or in terms of less structured interactions;
- States policies governing the assignment of entities to community roles.

A community contract thus provides a template for the instantiation of many community instances, each of which has characteristics and attributes stated in the community contract.

It is important to state that a community defines a context for defining business processes, structures and policies and can be regarded as a stronger form of UML use case models [UML].

3.3.5 Policy

A community *policy* constrains the behaviour of one or more roles in a community. The purpose of policies is to address uncertainty in the world of imperfect information and thus increase trust among the actors involved. For example, well-developed privacy policies in e-health will help to increase trust of individuals in the confidential use and disclosure of health information.

Multiple policies can apply to individual roles and there may be circumstances that require dealing with possible conflicts and resolving them (see section 3.4.2 for possible approaches to addressing conflict resolution3.4.1).

This version of the OIF proposes three *core policy types*, namely obligations, permissions and prohibitions.

O*bligations* specify a required behaviour.

Permissions specify behaviour that is allowed to occur.

Prohibitions specify behaviour that must not occur.

These basic policy types form the basis for expressing more complex organisational policy types such as delegation, accountability, privacy and consent. In addition, a community can specify violation conditions and possible penalty measures.

The power of explicitly defining policies and linking them to the behaviour of roles in the community lies in the fact that they can be changed during the lifetime of a community or can be tailored to a range of different e-health systems. Policies can be considered to constrain choices available in basic behaviour specified as part of business processes. This approach ensures a long lasting specification framework, supporting adaptability and evolution of systems in response to external (or internal) factors.

Policies can also control changes in communities, e.g. define which role in the community has an authority to change, update or remove other policies, define new roles and so on.

Note that some of the organisational policies will serve as a basis for specifying one or more information or technical policies that in turn apply to IT systems used in support of e-health services. An example of technical policy specification is Web Services Policy Framework [WS-Policy].

3.3.6 Business process

A *business process* is a structured style of behaviour usually described in terms of a number of related concepts, including:

- the constituent *business steps*;
  - each business step can have one or more *input artefacts* and one or more *output artefacts*;
  - these steps can be atomic in that they can not be decomposed into other business steps; these kind of business steps are referred to as *business functions*;
  - they can also be composed of other business steps or separate business processes; the constituent processes are sometimes referred to as *sub-process*;
  - they may be assigned to roles which are responsible for the enacting of the step.
- *control flow* between business steps, which can support sequential and parallel execution of business processes and make use of different types of control flow operators;
- *data flow* between business steps, describing how information artefacts are passed from outputs of one (or more) business step to the inputs of one (or more) other business steps, dependent or independent of control flow;
- *refinement operators*, describing how one business step can be implemented as a separate, lower level business process.

Therefore, a business process represents a specific style of behaviour where the focus is on flow of data and control and the roles involved may or may not be identified, depending on circumstances.

3.3.7 Domain and Federation

The OIF defines two special types of communities.

One type, called *domain*, distinguishes between two kinds of roles, namely the roles with certain controlling authority over other roles. Examples of domain communities are security or management domains.

Another special type is called *federation*, allowing peer-to-peer linking of domains. The usual way of facilitating federation is by establishing a service level agreement (SLA) between the controlling objects of the two domains. The SLA constitutes a federation community contract.

Figure 7 shows domain and federation communities. The controlling roles are shown as thick circles while the controlled roles are shown as dashed circles. The SLA is shown as a double line connecting controlling roles.

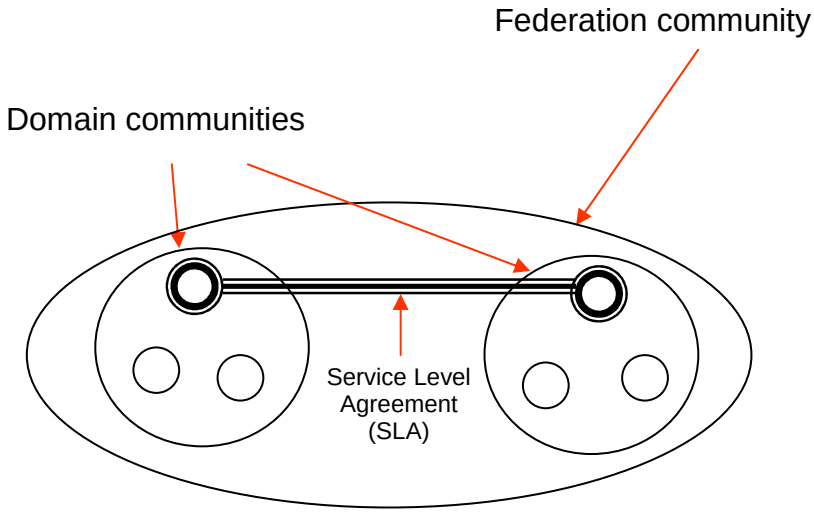

Figure 7: Domain and Federation communities

3.3.8 Business Service

A business service in the OIF is a particular abstraction of behaviour expressing the guarantees of service providers. Typically such guarantees are expressed in terms of service offers which, if accepted by service users (as a requestor for service delivery) form the basis of a service level agreement.

The guarantees involve policies that apply to the service providers (a special kind of party, see section 3.3.9) and, if a consumer accepts the service offer, certain policies are also applied to the consumer. This represents the formation of a service level agreement or a contract, typically with certain legal weight.

It is important to note that service delivery also involves benefits that service usage brings to service users and together with the cost of using the service, the value represents a factor in users deciding about different service offers.

3.3.9 Accountability concepts

The OIF also includes several concepts for accountability as follows [ODP-EL].

Party is a special kind of entity with emphasis on its legal requirements.

Delegation is the action that assigns authority, responsibility or function to others.

Principal is a party that has delegated authority, responsibility or function to another party.

Agent is a party that has been delegated authority, responsibility or function.

3.3.10 Evaluation

Evaluation is an action that assesses the value of something.

The value is linked to the notion of quality that in health has the dimensions of safety, effectiveness, patient centeredness, timeliness, equity and efficiency.

3.3.11 Location

Location is an important concept needed for describing various organisational relationships. They can have spatial characterisation as in the expression of how various artefacts or actors are assigned to physical locations or temporal characterisation as in scheduling actions for clinical treatment.

Location can refer either to space or time.

Location in space is an interval of arbitrary size in space at which an action can occur [ODP-RM].

Location in time is an interval of arbitrary size in time at which an action can occur [ODP-RM].

3.3.12 Distribution

This concept describes the assignment of artefacts, actors, resources or services in terms of different spatial or temporal locations. For example, one might maintain the definitive copy of a clinical document artefact in a repository of electronic health records at a particular location (e.g. a GP's practice). Another example is the location at which an actor or service performs a business step in a business process because it can affect a set of legislative policies that apply. In terms of resources, it is often required to have a precise knowledge of which resources are available at certain locations, e.g. how many and which GPs are available in a certain remote health service district. Note that distribution is often constrained by community policy.

3.4 Patterns

As noted in section 2.3.2, interoperability patterns are a mechanism for capturing existing knowledge and observations about commonly occurring phenomena in e-health.

From an organisational perspective, these include frequently recurring organisational structures, common modes of organisational interactions or processes and various kinds of legislative or organisational constraints and policies. Capturing these patterns will promote reuse of organisational interoperability approaches and ensure consistency across NEHTA's outcomes (and subsequently outcomes within the broader e-health community).

The organisational patterns make use of the core organisational concepts, introduced in the previous section. The patterns bring a pragmatic approach to addressing specific problems directly reflecting e-health concerns, while preserving precision and compatibility of expression owing to the use of well-defined modelling concepts.

Four high-level categories of interoperability patterns have been identified in the IF1.0:

- legislative/regulatory,

- governance,
- value assessment, and
- change management/education.

The IF2.0 provides refinement of the organisational patterns from the IF1.0 through the identification of a number of specific organisational patterns within the existing pattern categories which were thought to be sufficiently common to many e-health situations, in particular after considering a number of e-health projects. These patterns follow the pattern form introduced in section 2.3.2.

The IF2.0 also provides extension of organisational patterns from the IF1.0, through the inclusion of new categories of patterns, with the corresponding patterns, namely:

- certification,
- monitoring and auditing,
- corporate knowledge/memory
- standard business processes.

Considering the evolutionary character of the NEHTA IF, it is anticipated that new organisational patterns will be further identified and documented as they emerge.

3.4.1 Legislative, regulatory and enterprise policies

This category of patterns captures the key characterising features of national and jurisdictional laws and regulations and positions them in relation to the core OIF concepts.

Legislative and regulatory constraints need to be well understood and addressed for the design of e-health systems to enable organisational interoperability across health organisation boundaries and between jurisdictions. In addition, e-health systems should be designed with the expectation that the legislative and regulatory policies are likely to be occasionally revised and the e-health systems should be resilient to such changes.

Examples of such constraints range from different federal, state and territory legislation and policies (and their interplay) to international policies such as for example the US/AU Free Trade Agreement. The impact of these policies needs to be well understood and addressed within e-health systems.

The administrative boundaries above need to be recognised to support description of well-defined and structured interactions between communities. It is important to state that these boundaries are flexible and can change to support various kinds of emergent behaviour within the communities or to adopt new policies from the environment.

The key OIF concept underpinning the legislative and regulatory issues is the concept of *policy*. In addition, the pragmatics of enterprise modelling requires an accompanying framework for describing policies and their relationships as well as processes for managing them. This is because policies represent the rules and norms underlying each of the legislative and regulatory aspects.

In addition to the core policy concepts of permissions, obligations and prohibition, a policy framework will need to support the expression of other frequently used policy statements such as responsibility, rights, liability, consent and a number of privacy related constraints. These are more complex policy constraints that can be expressed using an appropriate combination of the core policy concepts. One pragmatic approach for expressing these constraints is by treating the complex policy expressions as special kind of interoperability patterns.

Two policy patterns were identified and presented in the interoperability pattern form, as described next[12].

Note that this section introduces an informal visual notation for describing policy patterns[13], as follows:

- Pattern definitions are depicted as dashed ellipsis, and the use of core policy concepts is shown as dashed arrow;
- The roles are shown as hexagons
- The core policy concepts are depicted as boxes and dashed lines depict how they apply to the roles
- Actions are depicted as triangles and full lines depict association of the roles with the actions
- The use of a pattern (defined previously) is shown as ellipsis (with full line).

Pattern name: Rights policy

DESCRIPTION:

Policy statements of rights are used in many situations in real life and in the legal sector to denote ownership, moral rights, copyrights, entitlements and so on. Rights are also used in the e-health sector to describe claims that have legal or moral justifications.

However, rights are often used interchangeably with the concept of permission although they involve higher complexity than permissions. Typically, they imply additional constraints on the behaviour of others in addition to the permissions for right-holders.

One category of such constraints refer to the *obligations* of others not to act in a way to prevent the holder of right from exercising them e.g. a GP is obliged to respect a patient's decision as to whether to undertake a surgery or not. These constraints are essentially *prohibitions*.

Another category refers to the *obligations* of others to perform actions for the benefit of a right-holder as in entitlement rights, e.g. a health-insurer is obliged to pay to the patient a proportion of the costs of medical services as per their entitlement (either as per public policy or private health insurance contract).

The purpose of this pattern is to provide description of rights in terms of an explicit core set of policies (as introduced in section 3.3.50, applying to the right-holders and other parties that are directly or indirectly related to right-holders.

SOLUTION:

This pattern is shown in Figure 8. The Organisational Rights pattern consists of the following elements:

- A role of *right-holder* (e.g. patient in a public hospital), a role representing the other *party* (e.g. doctor in an emergency department), and an *authority* role, describing the initial granting of the rights (e.g. government granting all citizens the rights to healthcare);
- a *permission* that applies to the role of right-holder to perform some actions

[12] It is anticipated that future versions of the IF will catalogue further policy patterns as the understanding of their positioning within e-health matures. For example, these include consent, liability, responsibility, accountability and delegation.

[13] A more complete pattern notation will be introduced in the next version of the IF.

- an *obligation* that applies to the role of right-grantor, with respect to the specified action;
- *action* to which the rights apply.

This pattern can be applied in a number of situations, to describe permissions, prohibitions and obligations associated with all parties involved in granting and respecting rights of right-holders.

EXAMPLES:

Rights to receive timely and adequate healthcare, rights to vote etc.

PATTERN CATEGORY:

Legislative, regulatory and enterprise policies

RELATED PATTERNS:

A further specialisation of this pattern is information rights as described in section 4.4.1

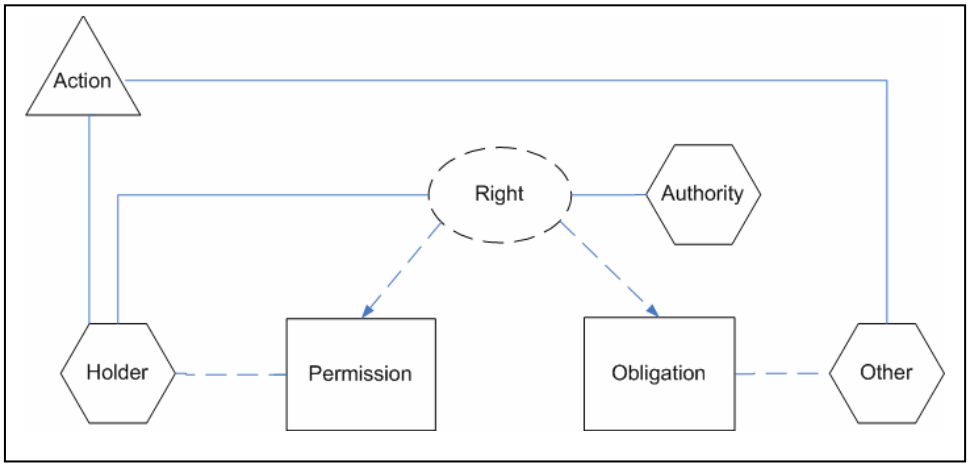

Figure 8: The Rights Pattern

Pattern name: Privacy policy

DESCRIPTION:

Privacy is an important aspect of e-health policy. The main application of privacy in health is in the policies that apply to personal and health information about an individual. These policies cover issues such as collection, access to, use and disclosure of information. There are other aspects of privacy such as physical or decisional privacy but they are not covered in this document.

One view of privacy is that it represents the degree to which an individual can determine which personal information is to be shared with whom and for what purpose. This is the view captured in this pattern. A more restrictive view of privacy refers to the ability of an individual or group to stop information about them from becoming known to people other than those to whom they choose to give the information.

The purpose of the Privacy pattern is to explicitly identify key policy elements common to many situations where privacy issues are of concern. This pattern can then be parameterised according to specific privacy concerns, e.g. a multitude of policy issues related to the Shared Electronic Health Records.

SOLUTION:

The solution (see Figure 9) applies to the first view of privacy above. Accordingly, privacy policy consists of:

- a right given to the individual

- to grant permission for accessing information about themselves
- to a selected other party.

Note that the figure depicts the *use* of the Right pattern defined previously, shown as ellipsis (full line).

EXAMPLES:

Privacy policies for accessing Shared Electronic Health Records

PATTERN FAMILY:

Legislative, regulatory and enterprise policies

RELATED PATTERNS:

This pattern makes use of the right pattern.

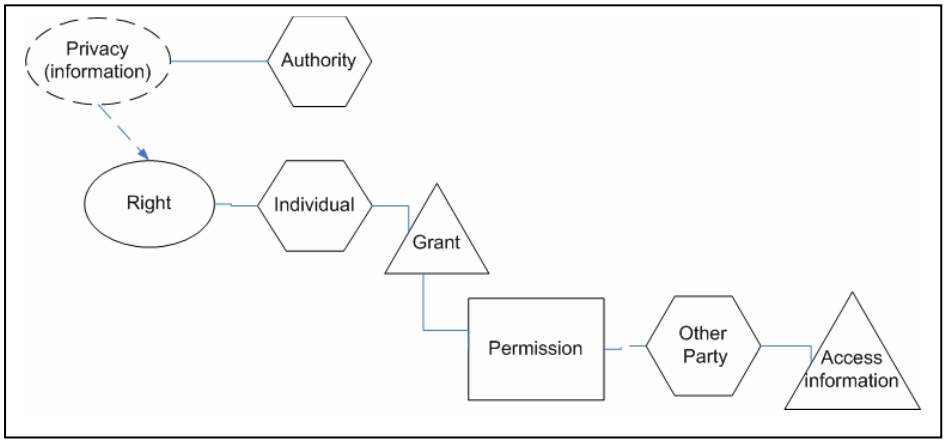

Figure 9: The Privacy Pattern

3.4.2 Policy conflict resolutions

This category of patterns is introduced to group different approaches to resolving policy conflicts. Policy conflicts arise either from the applicability of different sets of policies originating from different communities to an entity filling roles in these different communities, or from a new set of policies that may be introduced and be in conflict with the existing set of policies in a community.

This document captures two types of policy conflict resolution patterns, namely policy override and conflict mediation patterns.

Pattern name: Policy override

DESCRIPTION:

It is often the case that different policies apply to an entity filling different roles in different communities, reflecting the policies of each of the communities. As a result of different objectives of these communities and the different purpose of policies, there may be cases where conflicts between policies can arise. For example, an individual can restrict what personal information can be revealed to others, but secondary use requirements stated by governments may require access to that information for various epidemiological reasons.

SOLUTION:

One solution is to apply policy overrides, meaning that one set of policy takes precedence over another set, according to various legal principles (see [EDOC98] for more detail). For example, governments may

override certain privacy policy choices of individuals for the purpose of protecting public health. This pattern will require implementation of a policy enforcer component to implement application of the right set of policies and a policy manager component to support addition or change of policy descriptions.

EXAMPLES:

Detection of a highly contagious and/or communicable disease (e.g. bird-flu, measles) overrides privacy policy, but a less contagious disease may not, although this may trigger activation of a new policy.

PATTERN CATEGORY:

Legislative, regulatory and enterprise policies

RELATED PATTERNS:

Any policy related pattern (or concept).

Pattern name: Policy Mediation

DESCRIPTION:

This is the same problem as described in the above pattern.

SOLUTION:

The solution adopted in this pattern is to allow certain conflicts to occur. If that happens, mediation and dispute resolution approaches can be adopted as a way of addressing these conflicts. These are likely to involve escalation procedures ultimately involving a human decision maker in resolving conflicts. One such approach is presented in [EDOC03].

In both of these cases, the resolution can be applied by third parties or internally.

EXAMPLES:

Mediation authority to address complaints of individuals against healthcare delivery of a doctor.

PATTERN CATEGORY:

Legislative, regulatory and enterprise policies

RELATED PATTERNS:

Any policy related pattern (or concept).

3.4.3 Certification

This category of patterns can be regarded as a sub-category of governance patterns, but due to its significance, it is presented as a separate category. This category involves three patterns, namely conformance, compliance and accreditation.

A common solution to these three patterns can be to use the concept of community to represent the core solution to the problem. Therefore, three separate communities are introduced, i.e. conformance, compliance and accreditation communities, all of which provide a domain to which regulatory or legislative policies apply, while creating their own set of policies and processes.

This section presents the structure of the conformance pattern. The compliance and accreditation patterns have similar structure and they are given in more detail in chapter 6.

Pattern name: Conformance

DESCRIPTION:

When procuring products or undertaking acceptance tests, a number of checks can be put in place to ensure that the product or implementation satisfies its specification. The process of ensuring this is often referred to as conformance testing. This term is traditionally used in the area of testing products against a standard specification.

The main purpose of this pattern is to capture common roles, responsibilities and processes involved.

SOLUTION:

The solution adopted in this pattern is the definition of a conformance community. The objective of this community is to ensure well-defined and sustainable approaches to conformance certification. The community consists of the following roles:

- Conformance target (or tested system) – the artefact being tested;
- Tester - can be played by a human, or a machine, typically as part of a testing lab,;
- Reference point artefacts - the points where the tests will be applied;
- Certifier role - makes decisions about the outcome of testing and issues certification verification as written certificates or through other means;
- Control Board – meditates and resolves disputes.

The complete description of this community is given in section 6.4.3.

EXAMPLES:

Conformance of messaging products against HL7 standards.

PATTERN CATEGORY:

Certification

RELATED PATTERNS:

This pattern uses the OIF concept of community. Note that although the OIF treats community as the base concept, one can regard community as a pattern, providing a core solution for describing administrative boundaries with their constituent processes, strictures and policies.

3.4.4 Awareness and change management

This category of patterns is a necessary condition for:

- ensuring dissemination of best practices, standards, agreed approaches and new results/solutions into the national e-health community and
- implementing subsequent change management practices.

These are treated as two separate sub-categories, i.e. *awareness* and *change management*. This section identifies one specific pattern of the first sub-category, i.e. a dissemination pattern.

The approaches captured in this pattern category can be reused within different e-health projects or organisations to inform relevant e-health stakeholders about improved ways of delivering safer and more effective care. Examples of such new results and approaches are:

- Harmonisation of business processes in collaborative, cross-organisational and cross-jurisdictional environments, while respecting continuity of care and care continuum principles; the aim is to facilitate delivery of consumer-centric services;

- New management approaches that better focus on the needs of consumers, foster team efforts and encourage leadership; and
- The capabilities of new ICT technologies, paradigms and approaches, for example event-driven architectures, to address immediacy of information or workflow management systems to automate certain business processes.

Organisations such as NEHTA play an important role and complement market factors in increasing awareness and in educating jurisdictions about new business and technology approaches. In doing so, NEHTA has adopted a number of possible information dissemination approaches which can be contextualised through a dissemination pattern of the following form:

Pattern name: Dissemination

DESCRIPTION:

Organisational awareness about the benefits of new business and technology paradigms is an important factor when considering the e-health systems in the context of their *evolutionary* and *emergent* aspects.

The purpose of this pattern is to provide effective, efficient and continual dissemination of information about best practices, standards and new approaches to all e-health stakeholders.

SOLUTION:

There are three key parts to this pattern:

- Type of dissemination 'channels' for delivering information, such as Web, direct mail, or handouts at events;
- Type of medium for disseminating information such as online or paper documents, machine readable format, audio, video or presentation slides;
- Type of information that is distributed, such as e-health specifications, standards profiles, guidelines, and methodologies.

This structure allows the construction of certain specific solutions by combining these three parameters depending on the context, e.g. handout of e-health specifications using online documents at an event, or on the Web, or audio about some recent technology at an event, or on the Web.

EXAMPLES:

NEHTA workshops and jurisdictional/vendor events can be regarded as specific distribution channels using a combination of different medium types (typically slide presentations and handouts) to disseminate information and engage in discussions about e-health specifications or standards.

PATTERN CATEGORY:

Awareness

RELATED PATTERNS:

This pattern is using the technical pattern called service delivery channel (see section 5.4.1)

Once the benefits of standards, best practices or new approaches are recognised, *change management* activities need to be established to facilitate transition towards implementing new approaches or practices. This should be done on an ongoing basis to reflect new technologies or changes in the business environment.

A good example is change management associated with enterprise architecture developments. Its goal is to ensure that changes to the architecture are managed in a consistent way, allowing for flexibility in architecture evolution in response to changes in the technology and business environment.

Change management requires a combination of initiatives (government or organisational) and individual leadership to create a momentum for change. The initiatives aim at establishing governance structures, processes and policies to ensure controlled and evolutionary adoption of new technologies and management approaches. Leadership is needed to facilitate changes in cultures and mindsets for all involved in e-health – for the benefit of individual consumers, governments, service providers and vendors.

However, in implementing changes one needs to take into account risk factors such as those that potentially arise from new licensing mechanisms and operational policies in using emerging open source software.

NEHTA, for example, is established to facilitate an e-health transition within Australia, as part of overall health reform. Consequently, education and change management are high priorities within NEHTA as a way of influencing the community to implement similar approaches.

The organisational IF, through the concept of community, and through the policy-controlled techniques for changing community specifications, their structure, behaviour and policies, provides an explicit framework for guiding the process associated with change management. Thus, a special kind of community, i.e. a 'change management' community can be defined, specifying the roles with authority to undertake changes and the processes in which they are involved to do so. In many cases, such a community can overlap with the base community established to achieve the very objective of the community.

It is worth noting that business process reengineering has direct implications for change management. By providing a consistent approach to documenting communities and their constituents and behaviour, this may allow reuse of change management strategies across these communities.

3.4.5 Monitoring and Auditing

This category of patterns has a wide range of applicability for clinical, administrative and research needs.

Monitoring is the process of continual observation of a state or behaviour of some entity with the aim of recording information about or controlling that state or behaviour.

Auditing is a process of obtaining evidence about state history or behaviour trace of some entity, but as opposed to monitoring, this is not done on a continual basis but at certain points in time, after the event. For example, auditing is a specific area of concern for NEHTA's Identity Management initiative and the following text illustrates the context, purpose and solutions of this pattern [IdMResSet].

Pattern name: Auditing

DESCRIPTION:

> Health information about individuals is a sensitive artefact and its access needs to be controlled according to a number of policies such as confidentiality, privacy and consent. It is, however, possible that access to personal information violates such policies and the aim of auditing is to detect unauthorised information processing activities and record all user activities, exceptions, and events that should be noted for future investigation. It is to be noted that other kinds of information also need auditing, such as supply chain transactions and this pattern also applies to these situations as well.

The purpose of this pattern is to identify mechanisms for effective and efficient detection of many kinds of violations associated with access to personal information and other important information.

In terms of the application of the pattern, the auditing is likely to be initially the responsibility of individual clinics and jurisdictions, but in order to be a member of the National E-Health community, a minimal requirement will exist to perform auditing of any services through which roles in the national e-health community are accessed.

SOLUTION:

The first principle adopted is that each business service which requires access to sensitive information will require some degree of auditing. To this end, the pattern implements key recommendations from relevant standards such as the AS/NZS ISO/IEC 17799:2006. According to this standard an organisation should comply with all relevant legal requirements for its monitoring and logging activities.

Thus, all systems that implement such business services are to be monitored and information security events should be recorded and the monitoring should be used to check the effectiveness of the controls put in place to meet the organisation's access policy model. Examples of such events are creation, receipt, maintenance, or transmission of sensitive information.

In addition, certain roles referred to as auditors, will be tasked with review of results of any anticipated threats or hazards to the security or integrity of personal health information and review anticipated results of uses or disclosures of such information that are not permitted.

Some auditing may be quite complex due to the policies applying to the information artefacts, e.g. privacy legislation requires fine grained logging of access to restricted records.

EXAMPLES:

Examples of the information that audit logging could capture are:

- User IDs;
- dates, times, and details of key events, e.g. log-on and log-off;
- terminal identity or location;
- Changes to system configuration;
- use of system utilities and applications;
- Files accessed;
- Network addresses and protocol;
- Activation and de-activation of protection systems, such as anti-virus system and intrusion detection systems.

PATTERN CATEGORY:

Awareness

RELATED PATTERNS:

This pattern is related to the privacy pattern to determine which information can be classified as confidential.

3.4.6 Standardised Business Processes

This category of organisational patterns captures a number of standard business processes considered important in facilitating interoperability between people, organisations and systems. It covers certain common clinical and administrative processes but can also address research-related processes as for statistical or epidemiology purposes.

In spite of the fact that many activities and processes for specific healthcare contexts (e.g. communication, exchange of documents, and collaboration between hospitals and GPs) have been developed and established to meet the same objective, i.e. quality and safety of healthcare delivery, there are significant variations in how they are implemented. Although each of the stakeholders should be able to tailor best practices to reflect their own abilities and constraints, there is a significant benefit in the standardisation of certain business processes.

The purpose of all patterns in this category is to deliver consistency, safety and effectiveness of healthcare delivery to individuals and efficiency in service provision for providers through standardisation.

Each pattern is described using business process concepts introduced in section 3.3.6, and other organisational concepts as necessary.

It is important to note that process standardisation can facilitate improving information and technical interoperability. Furthermore, processes are defined in the context of policies that affect the use of processes.

This version of the IF has identified several standard business processes, namely patient registration, referrals, medication management and clinical notifications. The first two of these processes are presented in the interoperability pattern form below[14].

Pattern name: Patient Registration

DESCRIPTION:

Patient registration is one of the most common administrative processes undertaken in many e-health contexts, e.g. hospitals, GPs and so on. Typically, it includes two sequential business steps upon an individual's arrival at a health organisation: collection of information about the patient and verification of the patient.

The purpose of this pattern is to identify common business steps and their ordering in order to perform patient registration activities.

SOLUTION:

This patterns consists of:

- Two business steps:
  - Collection of information
  - Verification
- Three roles involved in the steps:
  - Administrator, performing collection and verification business steps
  - Individual, who is not an active performer, rather an entity being referenced in the process
  - Registration system, which can be regarded as a resource.

This pattern needs to be parameterised by the specifics of the environment in which it is to be applied, in particular policies that apply to the roles.

EXAMPLES:

Registration for GP visits, emergency department or upon transfer between hospital wards.

[14] A detailed representation of these business processes requires the use of appropriate process notation, e.g. BPMN or UML Activity diagrams. It is anticipated that next version of the IF will have adopted notation for these and other organisational concepts.

PATTERN CATEGORY:

Standard business processes

RELATED PATTERNS:

This pattern will be used by many other business processes, such as referral, admission, transfer.

Pattern name: Referral process

DESCRIPTION:

When individuals require certain additional healthcare services to the one already delivered (e.g. GP visit) they are typically referred to other healthcare providers (e.g. specialist or pathology lab). The steps involved and the documents used are similar in many such transfers of care and their standardisation provides many clinical and economic benefits. However, currently, the use of different referral processes for essentially the same purpose of transferring care among healthcare professionals leads to many inefficiencies.

The purpose of this pattern is thus to identify key business steps and roles that are common to many referral processes.

SOLUTION:

This pattern identifies common elements of many referral processes and it consists of [RefLandscape]:

- Three roles:
  - Referrer provider,
  - Referred-to provider
  - Individual;
- Business steps undertaken by Referrer including:
  - sending of referral document,
  - handling of acknowledgments from the Referred-to provider;
  - receipt of Status report and Discharge documents from the Referred-to providers;
- Business steps undertaken by Referred-To provider including:
  - Receipt of Referrals,
  - Sending of Acknowledgements to Referrer,
  - Sending of appointment notice to Individual and to Referrer.
- Business steps undertaken by Individual, e.g.
  - Receipt of appointment notice
  - Confirmation of the appointment.

These business steps can be augmented with additional steps such as decisions about subsequent steps in response to certain exceptional circumstances e.g. abnormal result or report flagging in radiology controversial.

This pattern needs to be parameterised by the specifics of the environment to be applied, in particular the reification of Referrer and Referred-to roles (see examples below) and the policies that apply to these.

EXAMPLES:

GP to Specialist, GP to pathology, Specialist to Pathology, Specialist to Specialist referrals.

PATTERN CATEGORY:

Standard business processes

RELATED PATTERNS:

This pattern uses the Patient Registration pattern.

It is anticipated that this category of patterns will in future include some other standard business processes such as handling of discharge summaries, e-prescribing, and long living processes such as chronic management support.

3.4.7 Governance approaches and models

This category of patterns captures various issues associated with needs to establish control of organisational or technical processes in an organisation. The problem domain is divided in terms of corporate and technology governance. Note that this document does not identify any specific governance patterns. These will be documented in the next version of the IF. Typically, each health organisation will have corporate governance and depending on its size and technology maturity, it will also have one or more other, technically focused, governance structures.

3.4.7.1 Corporate Governance

Australian National Audit Office (ANAO) defines governance as "the process by which organisations are directed, controlled and held to account" [ANAO, p.6]. The ANAO notes that many people treat governance as a concept relating only to the operations of, and relationships between, a governing board, a Chief Executive Officer and Ministers. However, while these are important, public sector governance also relies very heavily on the systems, processes, policies and strategies that direct operations, assure quality, monitor performance, and help manage these parties' obligations to stakeholders. [ANAO, p.5]

The ANAO Guide sets out six core public sector governance elements [ANAO, p.7]:

- Accountability – an organisation, and the individuals that work within it, are responsible for their actions and decisions and subject to external scrutiny;
- Transparency/Openness – stakeholders have trust and confidence in the actions of an organisation and the individuals that work within it; Being open, through meaningful consultation with stakeholders and communication of full, accurate and clear information, leads to effective and timely action and stands up to necessary scrutiny.
- Integrity – an organisation operates in accordance with high levels of honesty, objectivity, propriety and probity in the use and distribution of public funds and resources;
- Stewardship – an organisation holds public resources in trust for the public, and public officials exercise their powers on behalf of the public;
- Leadership – an organisation has effective leadership which sets the tone of the organisation and assists it to achieve good governance; and
- Efficiency – an organisation is committed to the best use of resources to achieve its goals

Note that the elements above can be also be related to the concepts and patterns from the pattern categories of legislative policies, value assessment, change management and standard business processes. These relationships will be addressed in the next version of the IF.

3.4.7.2 Technology Governance

Technology governance in the health sector covers a broad range of technologies including specialised medical equipment and devices as well as many types of information technology assets. The main technology governance focus of e-health is typically related to IT governance and Architecture governance, [TOGAF8.1].

Note that each of these governance structures may exist at multiple geographic levels - global, regional, and local - within the overall enterprise

IT governance is concerned with two key issues, the IT's delivery of value to the business, and mitigation of IT risks. These issues map onto the following IT governance areas [IT Gov]:

- Strategic alignment, with focus on aligning with the business and collaborative solutions
- Value delivery, concentrating on optimising expenses and proving the value of IT
- Risk management, addressing the safeguarding of IT assets, disaster recovery and continuity of operations
- Resource management, optimising knowledge and IT infrastructure
- Performance measurement, tracking project delivery and monitoring IT services

Architecture governance is a special kind of IT governance related to enterprise architecture and other architectural development within an e-health organisation. It is defined as 'the practice and orientation by which enterprise architectures and other architectures are managed and controlled at an enterprise-wide level. It includes the following:

- Implementing a system of controls over the creation and monitoring of all architectural components and activities, to ensure the effective introduction, implementation, and evolution of architectures within the organisation
- Implementing a system to ensure compliance with internal and external standards and regulatory obligations
- Establishing processes that support effective management of the above processes within agreed parameters
- Developing practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organisation

It is important to emphasize that in many organisations IT governance is becoming a board responsibility as part of overall corporate governance. The governance of an organisation's architectures is a key factor in effective IT/business linkage, and is therefore increasingly becoming a key board-level responsibility in its own right.

In terms of e-health, these principles of accountable governance need to take into account the fact that e-health systems often span multiple organisational and jurisdictional boundaries. They need to support both operational and strategic administration of e-health systems, both of which will need to be compliant with legislative and regulatory policies that apply to them as prescribed by respective authorities. For example, the anticipated future IT governance of the SNOMED clinical terminology needs to incorporate the strategic administration of content. The governance body will need to take on an overall responsibility for the direction, management and control of its management organisation, while respecting international, federal and state legislation and regulation. However, it will also need to include operational governance such as defining processes and systems for terminology management and editorial control of terminology products as well as governing the development, maintenance, enhancement and production of a

health terminology, at global and local levels. The activities of the operational governance bodies need to be overseen by strategic governance.

3.4.7.3 Governance community

Governance models are a special kind of the organisational concept of community. A governance community is created with the objective of ensuring that the functioning of the controlled sub-communities are according to the set of policies of that governance community.

Each governance community defines:

- The objective of the community, e.g. an architecture governance community has an objective of alignment of IT with business requirements;
- Key roles in the community and their responsibilities, e.g. an architecture board one of whose responsibilities is ensuring consistency between sub-architectures of an enterprise architecture; some roles can be artefacts or resources, e.g. a repository that contains various artefacts (e.g. documents, policies, standards) to be used by various architecture-related roles in this community, e.g. a requirements manager, business architect, information architect and so on.
- Accountability policies for the roles, e.g. the architecture board reports to a CIO;
- Processes in the community, that need to be implemented to meet community's objective, such as registering, validating, ratifying, and publishing new or updated content, compliance and conformance assessment, performance monitoring and so on.

Examples of some governance communities are project governance models, enterprise architecture governance, certification governance (see Chapter 6) and so on.

It is important to note that clear governance structures are necessary but not a sufficient condition for a well functioning organisation. Good governance needs to be complemented with personal leadership qualities, as recently reported in McKinsey study [Oct 2005]. In part, this is also related to the education and change management issues discussed in the section below.

3.4.8 Cost and value assessment

The 'cost and value assessment' pattern category emphasizes the need for a sound organisational cost/benefit proposition that needs to accompany information or technical interoperability solutions. This category was initially motivated by the key findings of the Boston Consulting Group [BCG]. The BCG report identified key benefits and priorities for the national e-health agenda in Australia and recommended a clear business case with quantifiable, clinical or outcomes-based benefits for all e-health initiatives.

In this version of the IF, this category was given further prominence in response to recent work within NEHTA, related to benefits realisation studies [NEHTA BR].

This category thus documents key approaches in estimating costs and determining value of using ICT in the health sector, as well as approaches for assessing relevant parameters of deployed e-health systems. Note that the value can be a function of a (sometimes complex) chain of ICT and health services dependencies as impact of deploying an ICT system propagates through a network of multiple health systems. The aim of this category is that these tried approaches be made available for further application by individual initiatives either before or after deploying ICT for health applications.

The term 'benefits' has been taken to cover a broader set of parameters than financial benefits, such as cost-savings or improved efficiency. However, benefits also need to cover factors such as improvements in healthcare quality and safety such as the reliable transmission of alerts about patients' drug reactions.

This category can be subdivided in two broad sub-categories, namely *ex-ante* and *ex-post* evaluations.

The *ex-ante* sub-category includes methodologies and approaches for estimating benefits to be realised from the use of specific ICT systems, *prior to* the deployment of the systems, e.g. undertaking cost/benefits analysis when developing business cases for NEHTA initiatives. One way of doing so, is through applying appropriate economic models and tools for evaluating and comparing values of ICT benefits. Note that the approach based on the use of economic models is a new type of value assessment pattern, identified in this version of the IF. It is important that such an analysis adopts a shared cost/benefit approach in which the fact that certain levels of automation in one e-health project impacts other projects is taken into account, e.g. the benefits flowing from the adoption of health identifier technologies (i.e. the individual and provider organisation identifiers) flows on to shared electronic health record (SEHR) technologies. This is in line with the recent report by the Productivity Commission [PCReportAug05] stating that the existing 'silo' approach to this kind of cost and value assessment might inhibit efficient assessment of emerging inter-dependent technologies.

The *ex-post* sub-category covers approaches and guidance for evaluating the benefits of the ICT systems *after* they are deployed. The importance of these approaches was also highlighted in the Productivity Commission report, the findings of which were that there are currently inadequate measures for assessing the benefits of the implemented ICT applications within the health domain[15].

The OIF has identified several approaches for assessing the value of initiatives, including the benefits of ICT in e-health. They include:

- *Benefits realisation approach* - a proprietary methodology, developed by the DMR consulting company [BRP]; this is used both for ex-ante and ex-post evaluations;
- The *IOM quality of care* framework, that provides a number of metrics for the measuring of quality of care [IOM]; this is used both for ex-ante and ex-post evaluations;
- *Influence diagrams* - a simple visual representation for identifying and displaying decisions, uncertainties, and objectives, and their mutual influence [InfluenceDiag] - exploited in the recent study which analyses the direct financial benefit of health information exchange interoperability between Australian healthcare providers and stakeholders [Sprivulis]; this is used for ex-ante evaluations;
- *Balanced Scorecard* methodology - enabling a clear definition of key organisational objectives, and their measures, that go beyond traditional cost-effectiveness measures; this is used both for ex-ante and ex-post evaluations; see for example the use of a balance scorecard in e-health as reported in [Ont].
- *Six Sigma* - has been applied in the health domain to improve quality and safety of care and address both clinical and operational issues. [SixSigmaH]. Traditionally Six Sigma was used for optimising processes that exists (i.e. ex-post), but newer extensions allow for the design for six-sigma (i.e. ex-ante).

[15] This is not only case in Australia but also internationally.

- *Prototypes* - to determine impact and effectiveness of new IT solutions and technologies as part of clinical IT development; this is used on the ex-ante basis.
- *Case studies* and *trials* - to determine benefits achieved and points of improvement; this is on the ex-post basis.
- *Value chain* for identifying discrete value adding functions in delivery of healthcare; one specific application is in analysing value that IT systems contribute to healthcare delivery as in [Porter].

It is anticipated that other emerging cost and value assessment approaches, such as a new business case framework being developed by the Commonwealth Government and tested by AGIMO, may influence NEHTA recommendations.

The OIF concept of community can be used to identify and calculate value that an ICT system delivers as part of the healthcare services delivery chain. This can be done through:

- Considering the system under consideration as assigned to a *supporting role* within a *community.* The community will consist of this role and the roles of various stakeholders involved in delivering healthcare services while using the ICT system, directly or indirectly;
- Such an ICT system's *behaviour* will be abstracted in terms of *services* it provides to objects filling the other roles in the community and who obtain *value* from using this system; the value, for example, can be considered in terms of increased safety, improved effectiveness, efficiency or timeliness in health service delivery; and
- If an ICT system is also part of *another community* (e.g. a health provider identifier system used within a SEHR community), the services that this system delivers also need to be considered in terms of the *value* the system delivers to the objects in the other community.

The resultant structure could be considered as a *value chain* that points at the linkages between the ICT systems and the communities in which they exist, and to which they deliver benefits; it is possible to then apply any of the value assessment methodologies, e.g. influence diagrams, to such a value chain.

3.4.9 Corporate Memory

Experience has shown that in many cases organisations do not provide sufficient recording of important information and decisions, such as those that relate to information systems design, but also administrative or even clinical information and decisions. In order to address this problem, there need to be mechanisms to support the recording of critical information or decisions of organisations. Examples of such mechanisms are requirements repositories, containing business, functional or technical requirements, or enterprise architecture repositories.

3.5 Summary

This section provides a summary illustrating how organisational concepts can be used to represent several healthcare stakeholders involved in care delivery and how the organisational interoperability patterns mentioned in this section can be positioned in relation to them. It also provides a high-level mapping of the organisational concepts on the modelling concepts from the HL7 V3 Reference Information Model (RIM).

Figure 10 shows a Care Community. It's objective is to provide a context for reliable and safe delivery of healthcare services to the individuals. This community includes the roles of an Individual, an Individual Healthcare

Provider and Healthcare Provider Organisation. The last of these roles can be represented as a community in its own right, consisting of a number of different Healthcare Provider Roles.

In addition, the figure includes the role to be filled by ICT systems to capture the use of various technologies to support the delivery of safe, reliable and efficient healthcare. This may cover one of more of the messaging services to support transfer of information, electronic health records, pathology systems, e-prescribing and so on.

The figure also shows high-level organisational patterns that, to varying extents, constrain the policies and processes of the Care Community. These patterns can be regarded as high-level communities. For example, state jurisdictions provide their own policies, as does the Federal jurisdiction and these together provide constraints for the functioning of the Care Community. Similarly, the policies and processes of other communities, i.e. Governance, Value Assessment and Education/Change Management communities can be applied to this community. Note that in these three cases these communities may be more tightly related to the Care Community, e.g. by having a common role specification between them. The figure also includes a Certification community, which can take one of the three specific forms, as detailed in chapter 6.

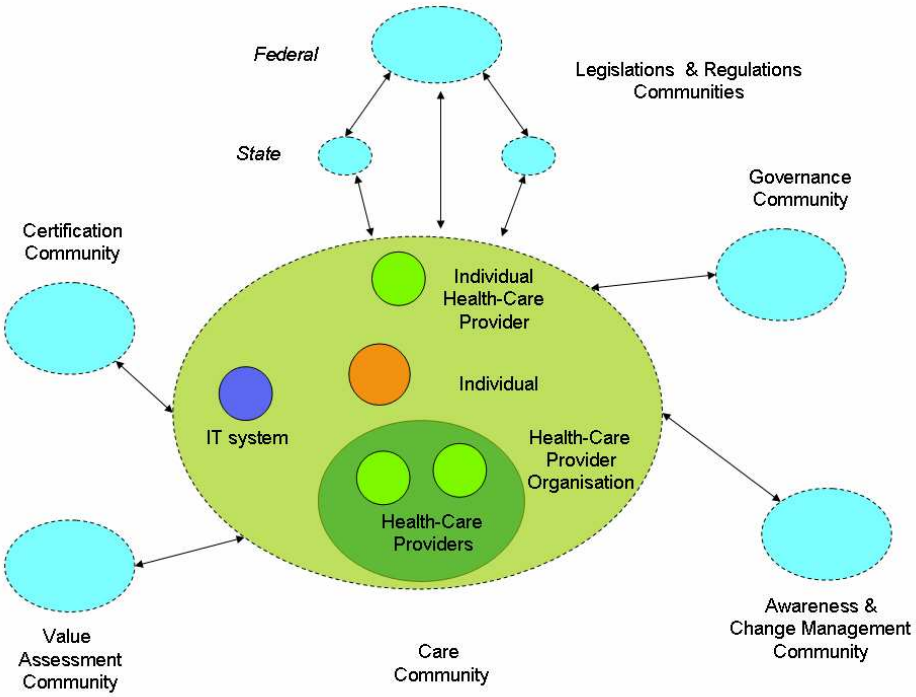

Figure 10: Care community – use of organisational concepts and patterns

The organisational concepts presented in this section can be mapped onto a number of modelling concepts proposed in the HL7 V3 RIM standard [HL7] – for the purpose of supporting these concepts as part of message exchange between health-sector participants. Some high level mappings are shown in the table below:

OIF concept	**HL7 RIM concept**
Entity	Entity (and its derived concepts, e.g. Person, Organisation, Place etc)
Community Role	Role

Action	Act (and its derived concepts, e.g. Observation, Procedure, ControlAct etc)
Actor, Artefact and Resource	Participation

Table 1: Some mappings between OIF and HL7 RIM

Note that the HL7 RIM does not have explicit support for the concept of community, policy, business process and business service, although the RIM concepts of Act, ActRelationship and RoleLink can be mapped to these organisational concepts for the purpose of supporting messaging. These mapping issues will be addressed in the next version of the Interoperability Framework.

4 Information Perspective

This section presents the information perspective of the IF, referred to as the Information Interoperability Framework (IIF). The IIF addresses the semantics of information of relevance for understanding, specifying and deploying e-health systems. The IIF allows for the description of key information components and their relationships. Typically the information components will represent certain artefacts in the organisational perspective. Note that the IIF is not meant to replace the existing information models or introduce a new information model but rather facilitate the co-existence of different information modelling approaches through a common reference point.

4.1 Background

This version of the IIF:

- adopts key information concepts from the IF1.0 and adds two new information concepts, *name* and *identifier*.
- refines information patterns and presents them in the interoperability pattern form and extends information in the pattern categories by introducing the meta-data category.

The next version of the IIF will be further expanded to reflect jurisdictional consultation and further work on NEHTA's initiatives as well as various international health informatics initiatives, including open standards such as HL7 [HL7] and SNOMED [SNOMED].

The IIF links the organisational perspective on interoperability to the information perspective. Relevant informational standards will be documented in the NEHTA Standards Catalogue (see Section 9).

4.2 Information Interoperability Principles

This section identifies a number of fundamental information principles that form the basis for the IIF. This covers:

- Separation of Information and Knowledge;
- Separation of representation form and interpretation of Information;
- Separation of Information and Data;
- Separation of formal concept representation and Clinical linguistics.
- Traceability from information concepts to organisational/technical concepts and patterns.

The first principle states that information and knowledge are distinct, although related concepts. We use the ISO standard [ODP-RM] as a basis of our definition of information, i.e.

> *Information is any kind of knowledge that is exchangeable amongst users, about things, facts, concepts and so on, in a Universe of Discourse*.

We take knowledge to mean an 'awareness or familiarity gained by experience, of a person, fact or thing', (Oxford Dictionary). Note that knowledge has an anthropomorphic nature and that its essence is about understanding of real world phenomena, which can be done through experience, e.g. through perception, learning through passing of information by others, or through a mental process. Not all knowledge is exchangeable, for example tacit knowledge.

The second principle states that information has a representation form. This is what makes information communicable. However, it is the interpretation of this representation (meaning) that is relevant in the first place [ODP-RM]. This is because the interpretation can generate some new knowledge. For example, through a medical observation process, a clinician captures key details about a patient, and records them using some representation form, typically written text (either in paper or electronic media). This capture forms information about the patient and the main purpose is to do some interpretation of what was recorded, i.e. patient diagnosis. This can be done by the very clinician who did the observation (based on his existing clinical knowledge) or after passing this information to other specialists for further observation and/or interpretation. It is through this chain of events that new knowledge (about health state of the patient) is generated.

The third principle further refines the second principle above, regarding the Representation Form of information and defining Data [ODP-RM], i.e.:

> *Data is the representation form of information dealt with by information systems or users thereof.*

Although in general, information systems can be any system which collects and stores information, in e-health, the aim is to represent data in an electronic form for subsequent electronic processing. An example is terminology inference as in terminology classifications.

The fourth principle is based on [Rector]. It states that, although formal concepts should be informed by clinical linguistics, they should be treated differently, because their users and their purpose are different. Formal concepts systems, such as various terminology systems (using different formalisms), have the purpose of machine-based processing and inferences of formal concepts, while clinical linguistics, has the purpose of expressing or understanding natural language concepts (i.e. words, lexicons, grammars) for the use of clinicians.

The fifth principle states that all information components represent entities from the real world as modelled in the organisational perspective; furthermore some information components will be used by technical components implementing business logic.

4.3 Core Concepts

An *information component* is the key IIF concept. This represents an element of information that corresponds to some concept in the real world, e.g. demographic information about an individual.

An information component can be:

- a simple, *foundation component* (based on standard data types, e.g. integer, string, date or quantity); or
- a more *complex structure* that consists of a set of information components such as contact details for an individual, or even Electronic Health Records (EHR).

A *relationship* between information components expresses some dependencies or associations between things in the real world that they represent. A special kind of relationship is a composition of several information components into complex structures as mentioned before. Another kind of relationship expresses *mappings* between different information components. These mappings can, for example, be used to assign semantic relationships between concepts or terms from different clinical term sets.

A *constraint* represents restrictions or rules that can apply to information components, such as a valid range of numbers representing blood pressure.

A *constrained structure* is a complex structure to which some restrictions or rules apply.

An *archetype* is a specific instance of a constrained structure, modelling clinical or other domain-specific concept by defining the structure and business rules of the concept [ISO/TC 215]. Archetypes may define simple constrained structures such as 'blood pressure' or 'address', or more complex constrained structures such as 'family history' or 'microbiology result'.

A *value domain* is another use of constraint. A value domain constrains data elements to a set of specific permissible values, e.g. severity can be restricted to be one of 'mild', 'disabling' or 'life threatening'. Another value domain constraint is the recommended use of concepts from a terminology, e.g. SNOMED CT.

In order to be able to refer to an entity in the real world (or to a concept), one needs the concept of name. *Name* can be defined as a term which, in a given naming context, refers to an entity [ODP-RM]. Nomenclature refers to a method of assigning names to entities as in Systematized Nomenclature of Medicine (SNOMED).

A related concept to a name is an *identifier*. It is defined as an unambiguous name in a given context [ODP-RM]. Examples of identifiers are those used to refer to individuals in a health context or to refer to health service professionals (both individual providers and organisations), as in the NEHTA Unique Health Identifier (UHI) project.

Finally, an *information model* will consist of a number of information components, to which various types of constraints can be applied and which are related to each other through different kinds of relationships. Examples of such information models are models for pathology, medications, immunisations, discharge and referrals.

4.4 Patterns

Information interoperability patterns are used to capture some common characteristics of information that are identified in various health informatics applications, both within NEHTA and jurisdictional efforts, and reused across them.

The information patterns will facilitate a shared understanding of important information concerns and approaches, and ensure consistency of NEHTA outcomes. They will also facilitate subsequent alignment within the broader jurisdictional community. The information patterns are described using the core information concepts, introduced in the previous section.

Five high-level categories of information patterns have been identified by NEHTA, as listed below. Considering the evolutionary nature of the NEHTA IF, it is anticipated that new patterns will be identified and documented as they emerge.

4.4.1 Information policies

This category of interoperability patterns refers to the recognition that there may be complex circumstances associated with the creation, access to, use and modification of information. In particular this refers to personal and health information about individuals or sensitive information about some medications or other medical products prescribed to an individual. This is particularly the case in modern healthcare environments in which there are many different parties that may interact with information components during their lifecycles and that information may be stored at various resources owned by many other parties.

A central concept underlying the existence of multiple parties and their involvement in the information life cycle is that of *rights* associated with

relevant information and corresponding obligations, i.e. *information rights*. This is a specialisation of rights patterns identified in the organisational perspective.

Pattern name: Information Rights

DESCRIPTION:

In a typical healthcare environment in which there are multiple parties involved in healthcare delivery there are circumstances in which they need to create, access, use, modify and transfer information.

The purpose of this pattern is to explicitly identify policies related to the rights for creating, using, accessing or modifying information, while taking into account the *Right* pattern defined in section 3.4.1.

SOLUTION:

This pattern is specialisation of the *Right* pattern from the organisational perspective and thus includes all the elements from that pattern.

In addition, it identifies different sub-patterns which describe the rights of different stakeholders involved throughout the lifecycle of information, including:

- Copyright;
- Moral Rights;
- Exclusivity;
- Access and Distribution rights;
- Modification rights; and/or
- Transferability of rights.

These different sub-patterns will be defined in more detail in the future version of the IF and presented using the interoperability pattern form, as required.

EXAMPLES:

This example illustrates the use of the different types of rights of a "data custodian" role for an Electronic Health Record Service, and one of the rights of the "individual" role.

The custodian for example:

- Does not hold the copyright or the moral rights (as these rights are exclusive and belong to the creator / author of the information);
- Does not have exclusive access to the information, as it may be shared with other people;
- Does not have the right to modify the information;
- Has the right to allow authorised third parties to access and redistribute the information, subject to appropriate permissions;
- Can under certain circumstances (e.g. termination of the EHR Service), transfer its rights to another EHR Service;
- may have rights to charge for information access (directly or indirectly).

In addition, the custodian

- has obligations to protect information;

Further, in this case, the individual:

- has rights to obtain access to their information based on freedom of information or privacy legislation.

PATTERN CATEGORY:

Information policies

RELATED PATTERNS:

This pattern makes use of the *Right* pattern defined in section 3.4.1.

4.4.2 Meta-data

This category of patterns captures common situations of using certain additional information to describe or define the information of concern. Accordingly, two patterns in this category are defined, as described in the following.

Pattern name: Describing meta-data

DESCRIPTION:

Many information components include information about the creator of the component, date, or version, and this type of additional information is referred to as defining meta-data.

The purpose of this pattern is to capture this additional information and distinguish it from the main content of the component.

SOLUTION:

The solution is to define separate information attributes associated with this additional piece of information.

EXAMPLES:

Version number of NEHTA Discharge Summary specification or 'data obligation' fields with it such as 'essential', 'desirable', 'optional' or 'conditional' attributes [Discharge].

PATTERN CATEGORY:

Meta-data

Pattern name: Defining meta-data

DESCRIPTION:

Many information components have defined structure which is typically done through the adoption of a schema that defines the structuring rules.

The purpose of this pattern is to capture this additional information for defining the information components and to distinguish it from the main content of the component.

SOLUTION:

The solution is to define a separate schema (or meta-model) which contains structuring rules for all information components that follow this schema.

EXAMPLES:

NEHTA Discharge Summary template [Discharge], XML schema defining structure of any XML document etc

PATTERN CATEGORY:

Meta-data

4.4.3 Temporal dependency

This pattern category is concerned with capturing the temporal dependency of information and taking this into account in the design and implementation of e-health applications.

In most cases, it is expected that such temporal properties can be expressed as constraints stated as policies in the OIF.

There are two patterns in this category, namely limited temporal validity of information and diminishing temporal relevance of information.

Pattern name: Temporal validity

DESCRIPTION:

In many situations information is of limited temporal validity, e.g. the expiration of referrals after 6 months from their issue. In many cases however, captured information may need to be kept indefinitely as it includes information about significant event occurrences that according to policy, must be archived. Examples of such long term information type could be genetic information, blood type, or allergies.

The purpose of this pattern is to ensure that, when accessing time-sensitive information, there is a mechanism for checking validity of the accessed information at a specific point in time. The specified time point for that information can be at the time of request or can be at any time in the past. If the time point is within the predetermined validity interval, it will be guaranteed that the information is valid at that point in time. For example, in scheduling a minor surgery for next week, a nurse can check the date when the last blood test was done so that if it is older than say 6 months, a new test needs to be undertaken.

SOLUTION:

The solution is to define a separate interface to all components where temporal properties are of relevance. In most cases, it is expected that such temporal properties can be expressed as constraints stated as policies in the OIF.

The interface is to provide an accessor function to get the value of the information component at certain point(s) in time. i.e. the accessor function includes a time parameter which specifies the time at which the value of the component is required. Note that this information can be used to trigger certain activity, e.g. sending reminders that a regular check needs to be performed.

Specific examples of approaches to deal with temporal properties are given in temporal patterns proposed by Fowler [Fowler].

EXAMPLES:

Referral duration;

PATTERN CATEGORY:

Temporal dependency

Pattern name: Temporal relevance

DESCRIPTION:

The nature of medical information is such that often information is of decreasing relevance with respect to time. For example, clinical information containing diagnosis results such as CT results may be obsolete after one year because new symptoms may occur in the meantime. At the extreme end, some information has no significance at

all after a certain amount of time, e.g. information about localised infection that has been cured or a broken toe that has healed.

The purpose of this pattern is to ensure that when information is accessed, there is a means of determining when information was recorded.

SOLUTION:

The solution is to associate a time stamp of creation of information with all information components where information may be of decreasing relevance, and provide a method of accessing that time stamp.

EXAMPLES:

Entries of most information in an electronic health record;

PATTERN CATEGORY:

Temporal dependency

4.4.4 Information quality

This pattern category emphasises the need to consider various aspects of information that reflect its fitness for use, or quality. This is of relevance for designing information quality goals and measures such as in maturity modelling.

Pattern name: Information Quality Characteristics

DESCRIPTION:

In general, quality is a multi-attribute variable consisting of several quality characteristics, such as:

- *Accuracy* - how well information represents a real-world value or thing for a particular purpose, e.g. how accurate is blood pressure information taken from a home BP monitor against that taken by a GP[16].
- *Access control granularity* - the precision with which access control policies are specified (e.g. only those who have rights to access information are permitted to do so)
- Accessibility - the ease with which information can be accessed.
- *Relevance* – information is only relevant within particular contexts, requiring identification of such contexts.
- *Fitness for purpose*– information should be written to suit the context, intention and audience to enable ease of understanding; for example, there is often a significant barrier between the understanding available to a consumer and that perceived by a medical professional.
- *Consistency of representation* – as information propagates across many systems, it can be transposed between representations by various messaging and integration hubs, losing a consistent representation and making future comparison and merging difficult. Note that information merging is a topic in its own right and is not addressed further in this document.

The main purpose of this pattern is to document common quality characteristics of e-health related information. The initial list of quality

[16] Note that in this example a home monitor may not be as accurate as that measured by a clinician but it may have the level of accuracy required for the purpose for which it is intended.

characteristics identified above is anticipated to be updated as new characteristics are captured.

SOLUTION:

The solution is to provide a separate interface to an information component that consists of methods for defining quality characteristics and accessing the value of these characteristics at certain points in time, as identified above.

This pattern can be extended to provide additional interfaces which can provide a specific range of values for quality characteristics of information components. These in turn can form the basis for setting up quality of service contracts.

EXAMPLES:

Graphical resolution of CT images;

PATTERN CATEGORY:

Information Quality

RELATED PATTERNS:

Temporal validity.

Pattern name: Measuring Information Quality

DESCRIPTION:

Improving the quality of health information is one of the key business objectives in the health sector in general and in e-health applications in particular.

The purpose of this pattern is to provide a solution to measuring information quality, which can be used to determine whether certain quality improvement milestones are reached.

SOLUTION:

The solution includes:

- An interface that provides methods for accessing specific fields within information components to allow access to the measured quality attributes; often, this would require measuring quality attributes at certain points in time, where quality has a temporal dependency
- A component that logs relevant information and, as needed, calculates cumulative or average quality parameters

EXAMPLES:

Measuring of accuracy of blood-test results;

PATTERN CATEGORY:

Information Quality

RELATED PATTERNS:

This pattern uses Information Quality Characteristics patterns.

4.4.5 Scope of application

This group of interoperability patterns captures the multiple uses applied to one piece of e-health information, e.g. clinical, statistical/epidemiological, or financial.

For example, during and after an inpatient episode the following information may need to be used or collected:

- For clinical purposes, throughout the process of health service delivery, health-care professionals can collect some information as part of a diagnostic phase. They may require access to other information (e.g. from the evidence-based knowledge repository) while they also create other clinical information while following a recommended care plan, including medications used.
- For financial purposes, hospital administrators need to create billing information, such as the cost associated with the hospital stay, but also the cost of health-delivery services. This information is used for billing and claims but also for checking budget compliance.
- For statistical/epidemiological purposes, there may be requirements for the collection of statistical information about that individual and the care they received, e.g. information about the type of disease, their age, gender and demographics. This information may be needed (or in some cases required) by various government agencies or other organisations for research purposes such as determining trends in populations, or population health planning.

In general, the OIF concepts and patterns can be used as a guiding mechanism in understanding the nature of information's purpose and its scope of application. In this respect, information needs to be considered in the context of one or more organisational concepts and patterns, such as:

- Business processes where it is created or consumed;
- Business policies determining permissions, rights, obligations and consent constraints regarding information access and creation; and
- Relevant organisational patterns such as legislative, governance and policy patterns that may determine the scope of application.

4.4.6 Information transformation

This pattern captures the commonly occurring requirement that information often needs transformation from one form to another as it propagates through a health community.

One such pattern category is message transformation, as different systems require syntactic changes during the exchange process. Such a transformation engine is often a critical integration component within jurisdictional systems as many message formats are used by many different applications and organisations.

Another category is the transformation from machine-readable forms to human-readable forms. The former is more suited for automated processing while the later supports human integration into organisational processes. Technologies such as XML have often been chosen as an intermediate form that can be automatically rendered into a visible form through a standard template, or parsed within systems based on a standard and predictable format.

4.5 Summary

This chapter has introduced a number of core information concepts. The purpose of these concepts was to serve as a common reference point for facilitating the co-existence of different information modelling approaches. In the context of NEHTA's work program for example, this is of particular relevance for the Clinical Information, Clinical Terminology, and Share Electronic Health Record initiatives.

In addition, the section has identified a number of information patterns that were identified based on an analysis of frequently recurring approaches in these initiatives and in one specific jurisdictional project.

In short, the Information Interoperability Framework (IIF) addresses the semantics of information of relevance for understanding, specifying and deploying e-health systems. Typically the information components represent certain artefacts from the organisational perspective.

5 Technical Perspective

The technical perspective of the IF is referred to as the Technical Interoperability Framework (TIF) and is presented in this section. The TIF provides a framework for specifying functionality to be delivered by the technologies employed within e-health applications - but oriented to a business purpose, as documented by the organisational concepts and patterns.

The TIF provides a set of concepts and technical interoperability patterns which serve as a common denominator for a number of specific technical solutions that can be employed in e-health systems today or into the future. The TIF concepts and patterns are general in nature to ensure a common understanding of technical concepts in the long term. The TIF is not meant to replace or introduce new architecture models but rather facilitate the co-existence of different technical modelling approaches through common reference points.

5.1 Background

The TIF specifies elements of a technical infrastructure. *Component architectures* have driven infrastructure delivery through the functional capability of software components. The approach is technology-centric (although independent of any specific technology choices) and allows for the composition of components to deliver higher-order functionality. A similar approach is evident in systems implemented in low-level programming languages which utilise software libraries to meet more complex solution requirements. The glue between components is still based upon primitive, technically oriented software approaches.

The recent approaches towards a focus on *services*[17] are more closely aligned to business functionality rather than technical functionality and provide a coarser grain of capability delivery. Through this business alignment, policy issues such as security, reliability and other quality aspects can be described with more business relevance than if directly applied to primitive software components.

Figure 11 graphically describes the relationship between basic ICT infrastructure (software components), the abstraction to business services, a composition capability to support business processes and orchestration, and ultimate access through service delivery channels. This supports service provisioning, access and use, as part of delivering business value to the end-users.

While software components reflect the capabilities of underlying technologies, the services should reflect functionalities required by the business context, including the contained business logic. From the implementation perspective, services can represent a subset of component functionality interpreted in a way to reflect business needs. This is based upon a generic principle of separation of concerns, similar to separation between computational and engineering concepts adopted by the ISO ODP standards. This approach is also in line with the key tenet of a specific TIF interoperability pattern (the Service-Oriented Architecture (SOA) paradigm described below) – defining services as a unit of business functionality.

Further, the functionality of a service is specified in terms of a service interface that reflects the business context. Note that this does not preclude implementing SOA using an Application Programming Interface (API), a client-

[17] The concept of 'service' in this section refers to services in a technical sense – to be provided by some ICT system; they are a distinct but related concept to that of 'business service' introduced in the OIF section.

server architecture, or a three-tier architecture. The key characteristic of an SOA service is that, regardless of its implementation, it is specified in terms of a business need, not programming terms.

Finally, services can be composed into even coarser units to better support automation of certain service relationships needed, for example, to support business processes and collaborations. Examples of some specific ways of composing services are orchestration and coordination. There are a number of interoperability patterns that can be used to characterise specific styles of composing components and services, as well as their dependencies, and these are described at the end of this section.

This version of the technical interoperability framework:

- Identifies key technical interoperability principles;
- Adds one new concept: service interface[18];
- Updates existing technical patterns and presents them using the interoperability pattern form.

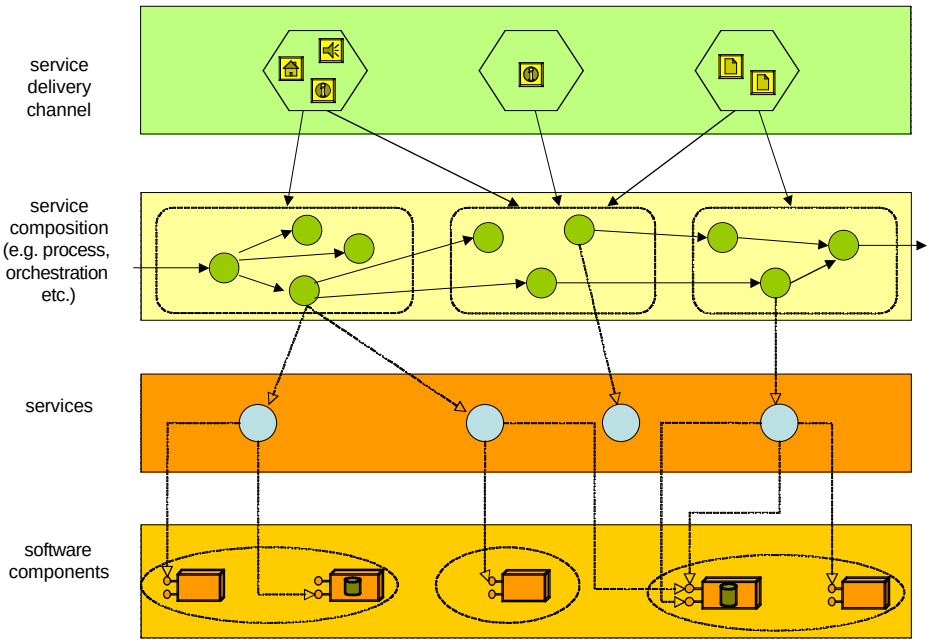

Figure 11: Relating business process to software components

5.2 Technical interoperability principles

The general interoperability principles from section 2.2.1 are refined and extended in the technical interoperability principles:

- Separation of technical specification from implementation
- Traceability of technical concepts to organisational/informational concepts and patterns
- Separation of policy description from implementation mechanism

This version of the TIF has taken into account NEHTA's work to date in technical architectures including Secure Messaging and more general technical principals and approaches from the ICT industry. The next version will be expanded to reflect jurisdictional consultation and further progress by NEHTA.

[18] This concept was mistakenly left out from the IF1.0

5.3 Core concepts

Software component – this is a software entity that makes one or more functions available to other components. Some of these functions or their aggregations can be used to support implementation of services.

Service – this concept is used to specify functionality of relevance for business; typically a service will implement the business logic of the corresponding OIF service description and can make use of one of more components. A service can also encapsulate existing applications.

Service interface – provides a mechanism for accessing functions provided by service.

Service composition – a way of establishing a behavioural relationship between several services, including various constraints on them, with the aim of supporting a more complex business activity such as a business process or business collaboration; there are various technical ways of composing services, such as orchestration and choreography.

Action – represents something that happens; for example a communication between two parties is considered an action as well as communication between two objects. There may be more than one object or party involved in an action.

Event – represents an occurrence of an action in the real world, typically indicating a requirement for some attention or serving as a trigger for initiating an interaction, performing a function or computation in an IT system. An event can be generated by actions of components or other actors (as defined in the OIF) or from the environment external to the components; a special kind of event is temporally driven, such as through time expiration.

Message – a unit of communication between software components, including those components that involve direct interaction with end-users.

Interaction – a set of related actions, which occur at two or more software components, or two or more services and which describe some cause-effect relationship between their behaviours.

5.4 Patterns

Technical interoperability patterns capture some commonly occurring, existing or emerging, structures, approaches and technical characteristics identified to be of importance for many enterprise systems. These patterns encompass service delivery channels, styles of component interactions, technical quality aspects and architectural styles as will be introduced below.

Some of these patterns have been identified through NEHTA's initiatives. In addition, the technical interoperability patterns will also need to include other types of interoperability patterns that capture broader knowledge of emerging technology trends such as event-driven architecture approaches. As with other IF components, the aim is to document the TIF interoperability patterns to support reuse across NEHTA's initiatives and broader e-health applications.

The technical interoperability patterns will facilitate a shared understanding of important technical concerns and approaches, and ensure consistency of NEHTA outcomes and subsequent alignment within the broader e-health community. The technical patterns are described using the core technical concepts, introduced in the previous section.

Several TIF interoperability patterns have been identified so far; they are described below.

5.4.1 Multiple delivery/access channels

This category of patterns is related to different types of delivery channels (from the standpoint of a technical infrastructure or service provider) that may be available to users for accessing the functionality of business services. Note that a business service is directly or indirectly implemented through one or more technical services.

The following different channels reflect specific technology options and can be provided as options to users. These options include:

- physical media (paper, x-ray film etc);
- electronic physical media (DVD, USB key or other token technology);
- connected interfaces (e.g. portal); and
- disconnected interfaces (e.g. local application).

Depending on the nature of the technology or business function in question, these service delivery channels can make use of one or more of the composition structures, services or low-level technical components. For example, a terminology service delivery can employ DVD technology or be delivered interactively through web-based portals.

Each channel has its own resource characteristics that may constrain the end-user experience. For example physical media represents a very different interaction paradigm than an online experience. It restricts the immediacy of updates and requires the delivery of physical media as opposed to online service access.

Portal interfaces are popular lightweight service access points utilising a web browser to provide ubiquitous access from a variety of platforms and locations. Such mechanisms have the potential to cover similar functionality to local applications but may restrict the breadth of the user experience depending on limitations in browser technology and interoperability.

Pattern name: Access transparency

DESCRIPTION:

The existence of different delivery channels provides flexibility to users in determining the one that best suits their requirements and abilities. However, multiple channel options also raise several problems in terms of ensuring consistent and seamless access to different business services that would otherwise require the use of several different access mechanisms.

The purpose of this pattern is to provide transparent access to business services, irrespective of a delivery or access channel.

SOLUTION:

One solution to this problem is provided through the Access Integration pattern, proposed as part of IBM's e-business pattern framework [IBM patterns]. This pattern enables access to business services or applications via multiple channels (devices) and identifies common services required to support a consistent user interface. In particular, the purpose of the pattern is to address the following common problems:

- Support access from multiple devices such as fat clients, browsers, voice response units, mobile devices, and PDAs
- Provide a common look and feel for all applications
- User-based customisation of presentation
- A single sign-on to multiple applications and information sources.

The pattern includes a number of technical services, i.e. Device support, Presentation, Personalization and Security and Administration. Further details can be found in [IBM patterns].

EXAMPLES:

- Thin Client and Voice-enabled Client for accessing services
- Single sign-on for seamless application access through unified authentication services

PATTERN CATEGORY:

Multiple delivery/access channels

Note that at the time of writing another pattern was considered but further analysis will determine whether this pattern is to be adopted. This is, what is referred to as a Personalised Delivery application pattern - allowing access to applications and information tailored to the roles of a specific user or group. Data collected can be related to application, business, personal, interaction, or access device-specific preferences.

5.4.2 Style of component interactions

This category of patterns covers the distinctive way software components can interact. The main interest in e-health applications is in the interactions between remote components (i.e. a distributed system environment), although the same principles apply for local (in memory) applications.

Several patterns are identified in this category and outlined below. Each of these patterns has its own technical characteristics that in turn makes it better suited for specific situations in support of e-health applications. Note that these patterns can be combined to define more *complex interaction* styles, combining the selected interaction styles with dependencies between the various component interactions.

Pattern name: Request-reply

DESCRIPTION:

Many distributed applications are based on an interaction model in which one software component/object requests another component/object to perform some function for it. So, there is single request and a causally dependent reply. One software object/component sends a message to another one, typically to perform some function and waits for the second object to reply with a result. This pattern is particularly common in client-server architectures.

SOLUTION:

Upon some business need, the requestor component sends a message to the responder component and then waits for the responder to perform certain processing. Subsequently, the responder sends another message typically carrying the result of the processing or certain notifications.

EXAMPLES:

Web Service calls over HTTP.

PATTERN CATEGORY:

Style of component interaction

Pattern name: One-way messaging

DESCRIPTION:

A component/object may need to communicate certain information to another component(s) but does not need to wait for any replies.

SOLUTION:

An object needs to implement a function where independent messages are sent to a nominated recipient with no expectation of a reply to the sender.

EXAMPLES:

WSDL one-way messaging.

PATTERN CATEGORY:

Style of component interaction

Pattern name: Publish-subscribe

DESCRIPTION:

Many business applications require an ability to be notified about certain important events as they occur. It may be that a single application or several applications are interested in the same event.

SOLUTION:

The solution is where independent events or messages are published by one application and received by zero or more (possibly anonymous) subscribers with no expectation of a reply to the publisher (i.e. undirected messaging);.

EXAMPLES:

Java Messaging Service (JMS) publish-subscribe.

PATTERN CATEGORY:

Style of component interaction

Pattern name: Continuous Flow

DESCRIPTION:

Some technologies such as multimedia require continuous flow of information (or sometimes referred to as streams) between components/objects (this is often referred as streaming).

SOLUTION:

The sender component/objects needs to provide a publishing function allowing that an ordered sequence of messages is directed to one or more downstream recipients.

EXAMPLES:

Video e-health applications such as tele-medicine.

PATTERN CATEGORY:

Style of component interaction

5.4.3 Technical quality

This category of patterns captures various problems related to technical quality, such as identifying quality characteristics, and solutions for defining and measuring quality.

In terms of the technical concepts, quality is of relevance for at least the service delivery channels, composite service structures, services and components, and their interactions.

Similar to the approach taken in information quality, the following technical quality patterns are identified.

Pattern name: Technical Quality characteristics

DESCRIPTION:

Technical quality is a multi-attribute variable consisting of several quality characteristics, such as:

- *Rate of information transfer*. This is a measure of the information exchange capability of system components. "Broadband quality" is often used as a benchmark for consumer access while industry is assumed to provide higher transfer rates.
- *Latency*. Information exchange latency refers to channel delay. The transfer rate may be high but higher latency can affect streamed communication including voice and video.
- *Probability of failure*. Failure can occur in different parts of a system including communication, storage, and processing. In many situations it is difficult to identify the exact point of failure but an overall quality measure of failure probability such as meantime between failure (MTBF) enables qualitative comparison of different component performance].

The main purpose of this pattern is to document common technical quality characteristics of relevance for interactions in e-health systems. The initial list of quality characteristics identified above is anticipated to be updated as new characteristics are identified.

SOLUTION:

Provide a separate interface to a technical component or interaction that consists of methods for defining quality characteristics and accessing the value of these characteristics (including at a specified point in time).

This pattern can be extended to provide (where appropriate) quality offerings of technical components, which can form the basis for setting up quality of service contracts

EXAMPLES:

Network bandwidth for exchange of clinical messages;

PATTERN CATEGORY:

Technical Quality

Pattern name: Measuring Technical Quality

DESCRIPTION:

Improving the quality of connectivity and interaction is an important enabler for communication between health professionals, which is one of the main business objectives in the health sector.

The purpose of this pattern is to provide a solution for measuring technical quality. This can then be used as a basis for determining whether quality improvements milestones are reached and what the points of improvement would be.

SOLUTION:

The solution includes:

- An interface that provides methods for accessing specific fields within technical components or infrastructure so that it is possible to measure quality attributes; often, this would require measuring quality attributes at certain points in time, where quality has temporal dependency
- A component that logs relevant events of technical significance and, as needed, calculates cumulative or average quality parameters

EXAMPLES:

Measuring actual rate of download of video information;

PATTERN CATEGORY:

Technical Quality

RELATED PATTERNS:

Technical quality characteristics.

5.4.4 Technical architecture styles

This category of interoperability patterns captures various approaches to combining and composing software components and their interactions, as previously described, into more complex structures for delivery of solutions. These approaches are characterised by different rules and constraints that guide such grouping, referred to as architecture styles.

Examples of such architectural styles are Service-Oriented Architectures (including older client-server architectures), Message-Oriented Middleware and Event-Driven Architectures (including Business Activity Monitoring specialisations). It is important to emphasize that a Service-Oriented Architecture style is more relevant to the relationship between business solutions and underlying technical delivery while Message-Oriented Middleware and Event-Driven Architectures are more closely aligned to a technical perspective.

Note that a specific e-health system may be built based on the application of one such architecture style or by combining several architectural styles in a consistent manner.

Pattern name: Service Oriented Architecture

DESCRIPTION:

In designing and supporting e-health applications it is important to understand the business benefits and expectations of the use of ICT to deliver safe and quality healthcare. In order to do such a design, there is a need to provide explicit identification of business services, business processes and described IT functionality in terms of support for the benefits.

The approach taken by Service Oriented Architecture (SOA) aims at establishing the alignment between business and IT. This is in spite of the heterogeneity of technologies and the different processes and policies involved in cross-organisational and cross-jurisdictional e-health systems.

The basic tenet of SOA is a specification of technical services that have a close link to business structures and processes and can be reused across several business application areas. The focus here is on identifying business units of functionality and capturing them in a manner independent of technical platforms or programming languages available or in use.

The purpose of the SOA pattern is to apply the key SOA principles to the newly developed e-health applications, and where possible to use them as a means of integration with legacy systems. The SOA style is regarded as an important pattern to realise a number of interoperability goals.

SOLUTION:

This SOA approach requires a looser coupling of applications and a higher degree of technical abstraction than has been the case in the past, in the client-server architectures for example. The focus of the

client-server architecture was on identifying building blocks as well, but these building blocks were limited by the structuring applied. It closely reflected a technology-driven (and not business-driven) view of applications.

An example of specific technology that can be used to implement SOA technical concerns is the Web Services (WS) stack. At present, many foundation technologies from the stack can be used to start providing SOA functionality, such as SOAP, WSDL and WS-Security. However, it is important to note that WS is the subject of many ongoing development efforts and their full compatibility with the SOA is anticipated to occur over next 3-5 years. In particular, one of the key impediments to the full SOA capability is policy-based management and control [Burton]. In spite of this, SOA is the best approach and most scalable architecture style today and WS's represent the most viable technical implementation approach.

Note that recent developments in SOA place more emphasis on the importance of policies. These (technical) policies define constraints and capabilities of a system or technical service. Similarly, the concept of business policy defined in the OIF is also considered a constraint, but applied to the behaviour of individuals or organisations. This similarity between the organisational and technical concept of policy will facilitate clear mapping between the two views of policies and subsequently between the business and technical views of services.

A SOA approach requires significant cultural change in the mindset of analysts, designers, and programers, who must start designing and building systems in terms of services that reflect business functionality needs, rather than being driven by the characteristics of available technical platforms.

EXAMPLES:

Web Services standards.

PATTERN CATEGORY:

Style of component interaction

RELATED PATTERNS:

Request-response; One-way messaging; change management;

Pattern name: Message Oriented Middleware

DESCRIPTION:

A certain class of e-health applications require reliable communications in spite of intermittent problems due to unreliable networks, casual users or timed connections. Message Oriented Middleware (MOM) is a technology that pre-dates SOA and has been used in many e-health messaging systems. It is worth noting that Web Services standards are increasingly addressing the space of reliability and transactions but they are either not complete or there is no significant commercial uptake of the related standards.

The purpose of this pattern is to capture the approaches adopted by MOM and reuse them either as part of forthcoming Web Services standards or as requirements needed for procurement purposes.

SOLUTION:

In traditional MOM, messages are usually addressed to their recipients indirectly through a message queue. This allows the sender and receiver to be loosely coupled, as they do not need to synchronise to communicate.

Direct addressing through recipient-named message queues may be less suitable for wide-area, large-scale systems and so it may be advantageous to decouple message sources and sinks with respect to naming, so they may be mutually anonymous to each other. This is often called a publish-subscribe mechanism although this name is more usually associated with Event-Driven Architectures (see the next pattern below). Sources "publish" to the entire network and interested sinks "subscribe" to messages. The network then only forwards messages if there is at least one subscriber waiting on that message queue [IEEE Distributed Systems Online].

MOM has a larger share of the market than Object-Oriented Middleware, being used for database access in large business applications.

EXAMPLES:

Examples of MOM are IBM's MQseries (reliable, MOM service) and SeeBeyond with their integration server (recently acquired by Sun Microsystems).

PATTERN CATEGORY:

Technical architecture styles

Pattern name: Event Driven Architecture

DESCRIPTION:

Many business services require immediate reaction to important business events. To facilitate this, an event-driven style of architecture can be designed.

Event-Driven Architectures provide solutions for those situations when it is important to express architectures in terms of events, their relationships and abstractions. They are chosen as an important pattern for many e-health applications and are expected to be applied more in future as the technologies and solutions in the area mature.

SOLUTION:

The key focus of the Event-Driven Architecture (EDA) is on events, either because they may trigger some application behaviour, or because one or more events together can signify some important occurrence of business value. EDA does not typically support a queuing metaphor as provided with MOM. Event generators publish event content and the event infrastructure will forward such content on to those event consumers who have indicated a need for that type of content. Event subscriptions tend to be content-based, providing an expression of interest over the entire event content. In contrast, MOM usually addresses message content to named message queues either representing subjects of interest or individual recipients.

Events are a more primitive level of behaviour than services, and signify an asynchronous style of behaviour. In contrast, SOA at present generally involves bi-directional request/response communications between an invoking and an invoked service. Both of these architecture styles will be needed for future enterprise systems.

EDA covers a number of areas, including:

- Event-driven processes which have the capability to react to external events, rather than to be driven by traditional local control and data flows; and
- Event correlation and abstraction, and other relationships between events such as causality, membership, and timing; these are needed to represent complex event patterns that may be used as part of event data mining to identify cause and effect relationships

between certain events, useful for example in detecting fraudulent and illegal actions.

EXAMPLES:

Business Activity Monitoring is a specific example of the use of EDA. It defines a particular use of event-driven processing to facilitate run-time monitoring of certain processes, activities, or people involved in business collaborations. This architecture style is, for example, employed in checking regulatory compliance such as Sarbanes-Oxley and HIPAA policies (United States).

PATTERN CATEGORY:

Technical Architecture Style

RELATED PATTERNS:

SOA

5.5 Summary

An overview of the key interoperability concepts and patterns presented in the previous sections is shown in .

Technical interoperability is sometimes regarded as the most important interoperability outcome if one approaches interoperability from an integration perspective. However this is not a correct interpretation of the IF's motivation or contribution. It is only as a complete set of interrelated perspectives that the IF value is realised.

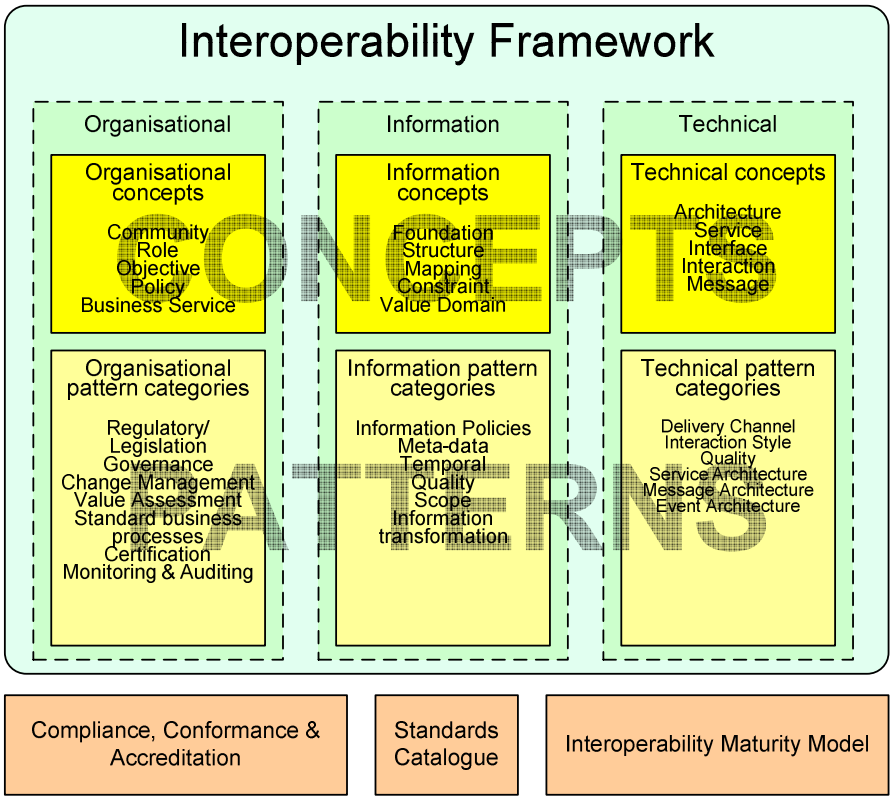

Figure 12: The NEHTA IF - key concepts and patterns

6 Compliance, Conformance and Accreditation

This section elaborates on the key ideas behind compliance, conformance and accreditation (CCA) and the accompanying certification processes, as outlined in the IF1.0.

In particular, this version of the Interoperability Framework:

- positions the CCA framework in relation to the IF,
- outlines key benefits of such a framework for various stakeholders in Australian e-health, and
- provides a clear description of the different roles involved in each of the compliance, conformance and accreditation areas, captured through their respective communities.

6.1 Background

An underlying principle of the medical profession is "First, do no harm"[19]. To ensure the fulfilment of this principle while considering modern technology as an integral part of the healthcare delivery chain, all efforts should be made to mitigate the risks associated with technology and the way healthcare professionals use it.

This "technology risk-mitigation" applies to the national e-health agenda and in particular to all stakeholders involved in healthcare delivery, including jurisdictions, vendors, health professionals, regulators and policy makers. There are two different, but closely intertwined, strategies for applying this principle in particular in the increasingly complex and technology-rich healthcare environment.

The first strategy is ensuring that *interoperability principles* are applied at the requirements and specification design stages, addressing concerns from organisational, information and technical perspectives. The interoperability concepts and interoperability patterns presented in the three previous sections are developed with that goal in mind.

The second strategy is *verifying* that the implemented systems satisfy the design specifications, that health professionals meet competence expectations for using the systems, and finally, providing assurances to all concerned to that effect.

In the Australian context, the first strategy is being embodied in the development and adoption of the NEHTA Interoperability Framework (IF). There is as yet no clearly articulated approach in the Australian context for the second strategy. The compliance, conformance and accreditation (CCA) framework presented in this section has been developed to support the second strategy.

A common feature of each assurance mechanism is that they encompass procedures for determining how well one component satisfies criteria contained within a specification. Consequently, these mechanisms are a special kind of *value assessment pattern*, identified within the organisational perspective of the IF.

Section 6.2 begins by highlighting the key benefits of the CCA framework for different stakeholders in Australian e-health. This is followed by the

[19] Famous Hippocrates maxim, 'Primum est non nocere', that became a guiding ethical principle in medicine.

description of the key role of specifications, including standard specifications, in defining fit-for-purpose systems and for subsequent verification procedures. The remaining part of this section provides a closer insight into each of the compliance, conformance, accreditation and certification areas and concludes with a list of required abilities needed to establish and sustain the CCA framework.

6.2 Benefits

This subsection is structured in terms of various stakeholders, all of whom benefit from a conformance, compliance and accreditation framework for health information systems.

6.2.1 Jurisdictions

State, territory and regional jurisdictions in Australia are major beneficiaries of a CCA framework providing them with:

- enhanced confidence in tendering processes by requiring of vendors that their systems follow architectural specifications (including open standards) which meet jurisdictional requirements; it is the specifications that dictate the system features rather than the available vendor offerings ensuring fitness-for-purpose of procured systems;
- more competitive procurement from the jurisdiction's point of view, giving them more control in the process of selecting the vendor who best meets their specifications;
- better assurance for interoperability within and across jurisdictional boundaries, including better plug-and-play capability of components; and
- satisfaction of economic and social constraints, such as ensuring that products deliver the expected benefits, but also provide better flexibility and reduced switching costs when replacing existing capabilities or when customising them for specific purposes.

6.2.2 Vendors

Vendors of health information and software systems benefit from a consistent and coordinated approach to e-health expectations, in particular in relation to a well-defined conformance framework including certification and accreditation approaches.

The following benefits are initially identified:

- Reduced cost and risk of delivering non-interoperable systems. Ensuring more predictable outcomes of engagement with jurisdictions and their own contractors and consultants – owing to a clearly defined set of procurement criteria;
- Better marketing of their products and their organisations;
- Differentiation in niche areas, allowing for enhanced competitiveness; and
- Improved customer relationships owing to more well matched customer expectations from clearly stated conformance requirements and vendor product certification.

6.2.3 Standards Development Organisations and Third Parties

Standards development organisations benefit by having a more viable business model reflected through the following activities:

- Serving as coordinators in developing standards while involving appropriate health experts and IT specialists, and setting rules for how conformance and compliance requirements are to be specified;
- Defining the range of acceptable measures and variations allowable for testing conformance and undertaking compliance audits;
- Providing services to guide specifications that are aligned with national and international standards; and
- Providing auditing services to check specification compliance with standards.

Benefits for testing labs and other third-party certifying organisations include:

- Providing competitive and differentiating services for independent conformance testing, compliance auditing and certification.

6.2.4 Users

Several types of users, grouped into the two categories below, will be beneficiaries of the certification program, once their respective requirements are met, namely:

- Physicians, hospitals, public health agencies and other healthcare providers, who can take a more active role in establishing the vision for future e-health systems and deriving the requirements to which manufacturers and regulators need to respond as argued in [Schrenker], and,
- Consumers of healthcare services, who will benefit from stronger management of transparency for their health information across various providers, jurisdictions and even the public-private boundary, in a reliable, accurate and secure manner. Ultimately, they will look for guarantees that the taxpayer's investment in IT systems is well spent.

6.3 Standards and Specifications

Standards and specifications are important elements in delivering an interoperable future. They support the separation of implementation from specification[20] allowing for component replacement and system evolution.

A specification is defined as "A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behaviour, or characteristics of a system or system component" [IEEE]. Typically, specifications are produced in a collaborative effort, involving different types of specialists and according to an established set of policies and processes. We refer to these roles, policies and processes collectively as a *specification community*.

The objective of a specification community is thus to deliver specifications according to the rules of the community. This community is a prerequisite for conformance, compliance and accreditation communities to be described in subsequent sections. Note that in the description of all communities, a specification is represented as a special kind of Organisational IF role, an artefact role.

6.3.1 Types of specifications

There are different types of specifications including:

[20] Occasionally implementation details and requirements may exist within architectural specifications but these situations are an exception rather than the norm and should be noted as exceptional cases.

- Solution specification: the specification of a special purpose IT system, such as the systems to implement an electronic health record (EHR), an e-prescription system, or a clinical information system (CIS).
- Standard specification: The specification of a more general purpose and endorsed by Standard Development Organisations (SDO), such as HL7, SNOMED or Web Services standards.
- Policy specification and regulations: The specification of rules and principles embodied in regulations, laws, and enterprise policies. Examples of regulations include HIPPA in the US and the Commonwealth Privacy Act in Australia.
- Competency specification: The specification of competency expectations for undertaking certain tasks, either of organisations to demonstrate their credibility, e.g. of testing labs to provide reliable testing capability, or of people (or systems) to demonstrate their skills, e.g. as expected of health professionals, or a Tester role in the conformance community (see section 6.4.3).

These different types of specification are the central point against which conformance, compliance or accreditation of a certain specification target will be assessed. For example, a conformance target can be a product, system or an implementation that needs to be tested for conformance to a specification. A compliance target can be regulatory and legislative policies, enterprise policies or other standards with which the specification in question needs to be consistent. An accreditation target can be a person whose competencies need to be checked against a position description specification (see Figure 13).

Accordingly, a specification is included in the specification community as an artefact created during the specification process. In each of the conformance, compliance or accreditation communities, this artefact is a central point for assessment (as will be described in detail in sections 6.4, 6.5 and 6.6).

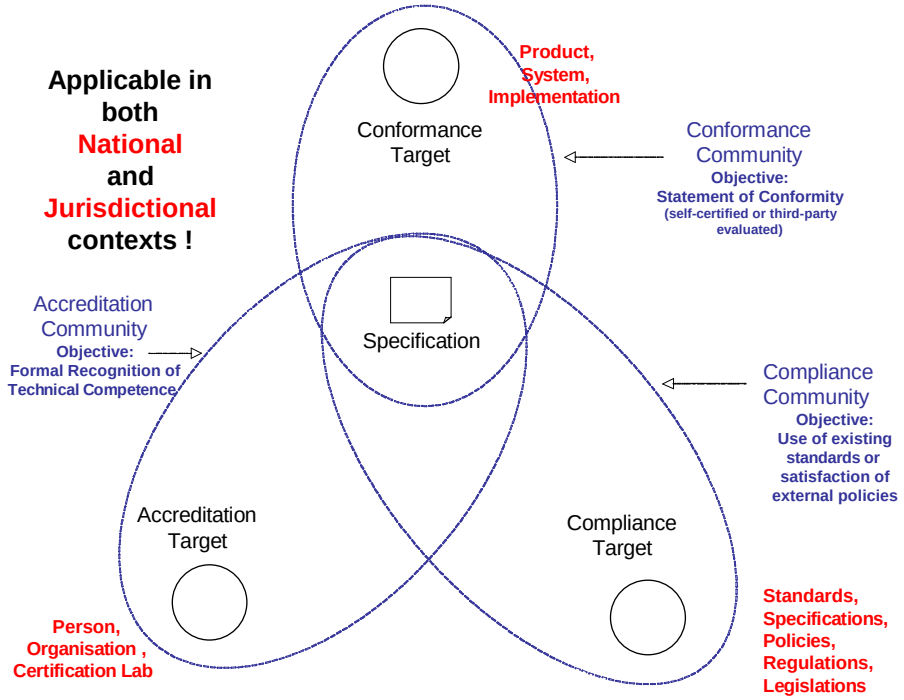

Figure 13: Conformance, compliance and accreditation targets for specifications

6.3.2 The Central role of specifications

The importance of specifications is in the fact that they are written to satisfy the requirements stated by domain experts. There can be many implementations fulfilling a specification. In general, it is expected that

specifications will change less frequently than implementations and that new implementations can be deployed for various operational or strategic reasons. However, even in cases where specifications change frequently in response to changes in requirements, there needs to be a clear traceability path from specification to implementation so that implementations correctly implement and support new requirements.

Specifications provide well-structured models of desired system behaviour and there may be many solution designs and respective implementations using different technologies to satisfy a specification. This can be achieved by either developing a new specification for new functionality as in Electronic Health Record (EHR) systems (which are yet to be implemented in many countries) or re-using existing specifications as in secure messaging or authentication technologies that are needed to support an EHR system.

Specifications can be structured in terms of organisational, information and technical perspectives for a particular system, but the system should not be considered in isolation from other systems. This is where an Enterprise Architecture provides architectural alignment between systems (and hence specifications), avoiding the 'silos' approach of the past.

A further role of specifications in future e-health systems is highlighted by the emerging trend towards the use of model-based tools, which utilise specifications in new ways. The electronic form of a specification makes it possible to analyse different models before they are deployed, to provide simulations and verification, including simulations of the effects of requirement and specification changes. Furthermore, the use of tools can provide a code generation facility, thus lessening the burden of system implementation and change. This is a significant shift from having specifications in only paper document form.

6.3.3 Specification community

Key roles in a specification community are (Figure 14):

- Specifier role – this will be filled by an actor who constructs a model of the expected system behaviour and of the behaviour required of its environment, i.e. an e-health system specification. This is based on a ser of requirements, including business, functional and clinical safety and quality requirements. In the case of NEHTA, for example, these can be specialists involved in producing specifications as part of NEHTA's initiatives. If conformance is required, this role also specifies conformance points in the specification, i.e. locations at which observation must be made possible in a conforming implementation.
- Approver role - has an authority to approve the specification.
- Stakeholder role (or sometimes called sponsor) - provides feedback to the specifier reflecting domain knowledge and requirements.

Figure 14 provides several examples of entities that can fulfil the roles in the specification community. For example, in the case of the Specifier these can be an Enterprise Architect, Solution Architect, Standards contributor or Policy maker, all of which are involved in creating specifications (of different types).

Note that a special kind of specification community is a standards specification community. It has its own set of policies and processes, reflecting a specific governance structure typical of many standardisation organisations (thus enabling its mandate in local, national and international arenas).

Recall that specifications are modelled as OIF artefact roles within the specification, conformance, compliance and accreditation communities.

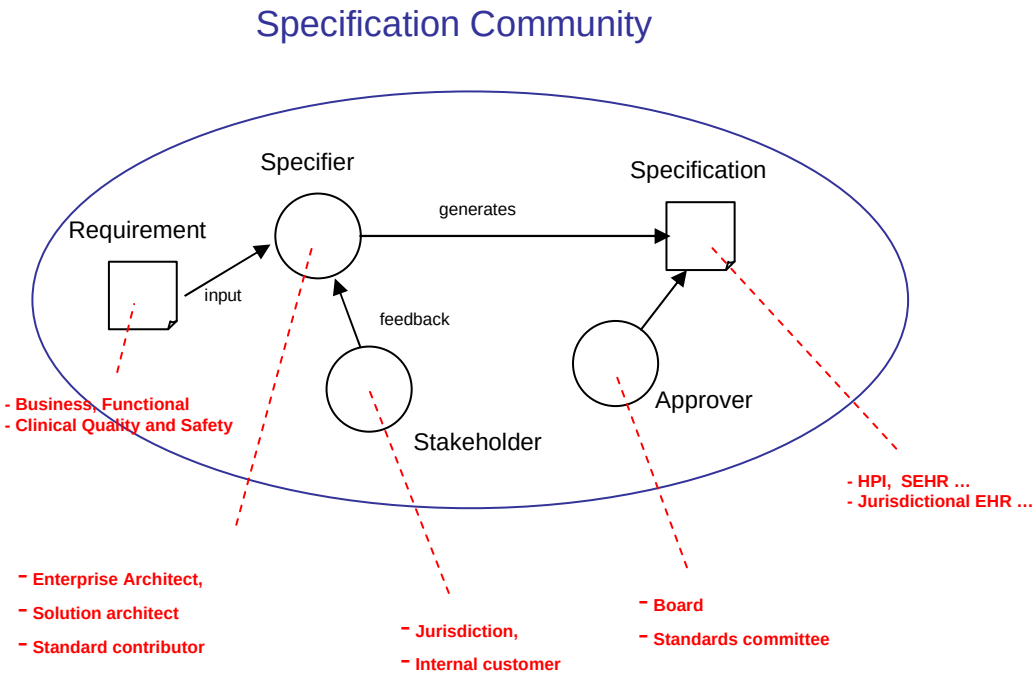

Figure 14: Specification community

In isolation, standards and specifications provide guidance for interoperability, but it is only through some form of measured adherence to these standards and specifications that the benefits will be realised. NEHTA's approach to express such adherence is through the use of two separate principles, namely compliance and conformance principles, following the ISO recommendations [ODP-RM], as will be presented in sections 6.4 and 6.5.

Specifications are of significant value in the interoperability process. In order to interoperate with other specifications, they should *comply* with openly available standards and define *certification points* through which *conformance* to the specification can be tested. These two points are elaborated in sections 6.4 and 6.5.

6.4 Conformance

6.4.1 Definition

Conformance relates an implementation to a specification (see Figure 20) whether or not the specification is a standard. (Further details about the various kinds of specifications are provided in section 6.3.1.) Conformance is checked based on the observation or test of an implementation/system according to conformance points included in a specification and compares these observations with the specification statement (conformance points).

This section first provides a definition of conformance points that need to be stated in specifications and how these can be used as part of conformance testing procedures. This is followed by a description of key roles and their obligations and permissions in a conformance community.

6.4.2 Conformance points

Conformance requires that any proposition that is true in the specification must be true in its implementation [ODP-RM]. A conformance statement is a statement that identifies *conformance points* within a specification and the behaviour that must be satisfied at these points. A conformance point is a

reference point where a test can be made to see if a system meets a set of conformance criteria. Conformance statements will only occur in standards which are intended to constrain some feature of a real implementation, so that there exists, in principle, the possibility of testing [ODP-RM].

The truth of a statement in an implementation can only be determined by *testing* and is based on a mapping from terms within the specification to observable aspects in the implementation.

At any specific level of abstraction, a test is a series of observable stimuli and events, performed at prescribed points known as *reference points*, and only at these points. These reference points are accessible interfaces for testing.

ODP standards define four classes of reference points:

- Programmatic - a point at which a programmatic interface can be established to access a function. The interface can be between application components or at a middleware boundary,
- Perceptual - a point at which there is some interaction between the system and the physical world, ranging from screen and keyboard interactions to process sensors,
- Interworking - a point at which an interface can be established to allow communication between two systems; an interworking conformance requirement is stated in terms of the exchange of information between two or more systems, and
- Interchange - a reference point at which an external physical storage medium can be introduced into the system, e.g. disk or other digital token.

6.4.3 Conformance community

The objective of a conformance community is to test and certify, as appropriate, software or hardware implementations against the specification for which they claim conformance. Conformance testing is often applied in the context of testing against standards and sometimes in testing against special purpose specifications (see Figure 15).

The following roles in the conformance community are identified:

- Conformance target (or tested system) role – for example, this can be filled by an Electronic Health Record (EHR) system, Health Provider Identifier (HPI) system or other systems to be produced according to specifications (including NEHTA specifications);
- Tester role - can be played by a human, typically as part of a testing lab (e.g. in the case of a perceptual reference point), or a machine (e.g. programmatic and interworking reference points); usually the tester role requires certain level of accreditation (see section 6.6 for more detail);
- Reference point artefacts - the points where the tests will be applied;
- Certifier role - makes decisions about the outcome of testing and issues certification verification as written certificates or through other means; this role can also perform registration of certified products; in the context of testing, certification refers to a specific product or implementation[21];
- Control Board – mediates and resolves disputes.

Note that a conformance community may include an additional role of regulator which selects a set of specifications against which a specific product needs to be assessed.

[21] Note that a different but related set of criteria need to be satisfied if an organisation is to be 'certified' for its competence, which is referred to as *accreditation* in this document.

The following processes and policies in this community can be identified:

- Conformance processes specify the steps involved in the testing and certification process. These are typically stated as part of conformance test suites, which are defined to facilitate testers' interpretations of the tested system observations;
- Policies that specify permissions, prohibitions and obligations of the tester role as part of the testing process; and
- Policies that specify permissions and obligations of the certifier role.

It is important to state that reference points can be chosen from either organisational, information or technical IF perspectives. For example:

- The interworking reference point (stated in terms of the exchange of information between two or more systems) can be used to test 'semantic' (as in information) interoperability conformance;
- A programmatic reference point is more about the functionality of a system and is of concern for the technical perspective, e.g. reference points in a Service-Oriented Architecture;
- A perceptual reference point can be considered from the organisational perspective but also from other interoperability perspectives.

It is possible to use the same testing structure, but different types of reference points, to test various IF perspective conformance.

Note that the conformance community above will typically involve additional roles such as an Owner role (representing any kind of stakeholder who is purchasing a system and who instructs the Tester role), various Liaison roles (e.g. with the specification community, or with vendors or jurisdictions) and a Community Governance role that sets the rules for the community and is involved in monitoring the activities and deliverables of the conformance community.

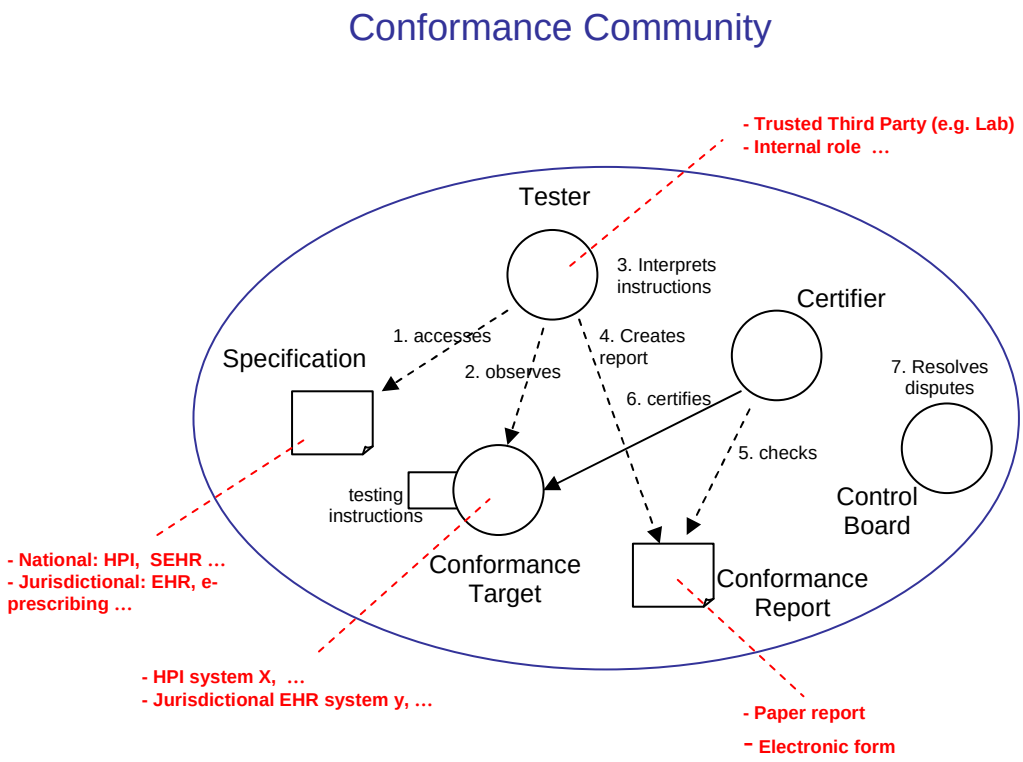

Figure 15: Conformance community

All NEHTA technical solutions will be required to conform to the specifications whether those implementations are provided through NEHTA or from external software vendors.

6.4.4 ISO approach to Conformity Assessment

In developing a conformance approach, NEHTA takes into account recommendations of the ISO Council Committee on Conformity Assessment (CASCO). CASCO is ISO's policy development committee on conformity assessment, reporting to the ISO Council [CASCO]. Its purpose is to encourage best practice and consistency when products, services, systems, processes and materials need to be evaluated against standards, regulations or other specifications.

CASCO makes a distinction between first, second and third parties involved in conformity assessment, namely [CASCO]:

- First-party assessment refers to the conformity assessment to a standard, specification or regulation carried out by the supplier organisation itself, i.e. a self-assessment. This is known as a supplier's declaration of conformity.
- Second-party assessment indicates that a customer of the supplier organisation carries out the conformity assessment. For example, the supplier invites a potential customer to verify that the products that it is offering conforms to relevant ISO product standards.
- Third-party assessment refers to the situation when a body that is independent of both supplier and customer organisations, e.g. a certification body, performs the conformity assessment. For example in ISO 9000 certification where an organisation's quality management system is assessed by an independent "certification" body against the requirements of an ISO 9000 standard. If the system conforms to the requirements, the certification body issues the organisation with an ISO 9000 certificate.

CASCO also defines additional assurance mechanisms that are worth mentioning. One example is Mutual Recognition Agreements (MRAs) formalised through cross-border cooperation among conformity assessment bodies and also among accreditation bodies. Through MRAs the parties involved agree to recognize the results of each other's testing, inspection, certification or accreditation. Since MRAs facilitate the acceptance of goods and services everywhere on the basis of a single assessment in one country, they contribute to the efficiency of the international trading system to the benefit of suppliers and customers. Australia's 1998 MRA with the European Union, for example, has led the way towards a more harmonised regulatory system, some of which includes pre-market assessment requirements such as conformance testing.

Another example is a Supplier's declaration of conformity (SDoC) that gives an option to a supplier to avoid the costs of third-party assessment. Such a self-declaration does not exempt the supplier from its responsibility to meet relevant regulations - for example, in relation to product liability. Such declarations generally need to be accompanied by effective post-market surveillance [CASCO].

Each of the CASCO assurance mechanisms is subject to the corresponding ISO standards. Note that the compliance issues as discussed in this document are not within the scope of CASCO activities because they position themselves within a conformance rather than compliance assessment role.

6.5 Compliance

6.5.1 Definition

One standard or specification is *compliant* with another standard or specification if all propositions true in the initial standard are also true in the complying standard. For example, the Web Services security specifications must be compliant with Web Service messaging (SOAP).

It is certainly possible to develop new specifications with no compliance to existing standards or specifications. However this is not the desired outcome. Existing standards or specifications should be referenced and adopted wherever possible to allow maximal potential for interoperability. Where no standard is chosen, there is little chance of two independent specifications sharing common approaches and thus enabling the use of common infrastructure.

The term compliance is also used to state expectations as to how certain specifications need to satisfy possible legislative or regulatory constraints or requirements as shown in Figure 18.

Compliance is an issue for all NEHTA specifications as well as any other specification referencing NEHTA specifications.

6.5.2 Two categories of compliance

There are two categories of compliance mechanisms:

- The assessment of specifications or standards in terms of how well they use or reference other standards, and
- The assessment of organisations in terms of how the policies and processes they put in place follow recommendations of some regulatory compliance policies.

An auditor role is common to both of these compliance aspects. The auditor's task is to check how well the assessment target matches the specification that is being referenced. For example, an independent auditor can check how internal policies and controls defined within healthcare organisations, with respect to their information systems, follow the rules and policies of HIPAA regulations. Similarly, an auditor can be engaged to inspect how a specification for an EHR system uses required standards, e.g. information security and privacy standards.

6.5.3 Compliance community

The objective of a compliance community includes checking whether specifications or standards correctly reference and appropriately interpret relationships to other standards as well as checking whether an organisation’s policies and processes follow the recommendations of some regulatory compliance policies.

Key roles within a compliance community (see Figure 16) include:

- Compliance target – these are the specifications of standards, or other specifications, that the specification in question references; or the external legislative or regulatory policies whose rules the specification in question needs to respect;
- Auditor - typically an independent third party who inspects a specification. These are mostly manual processes. An auditor follows auditing instructions to interpret the rules provided by a specifier and then records results of this interpretation in an audit (or compliance) report.
- Compliance authority - has the authority to decide upon the level of compliance as investigated by the Auditor.

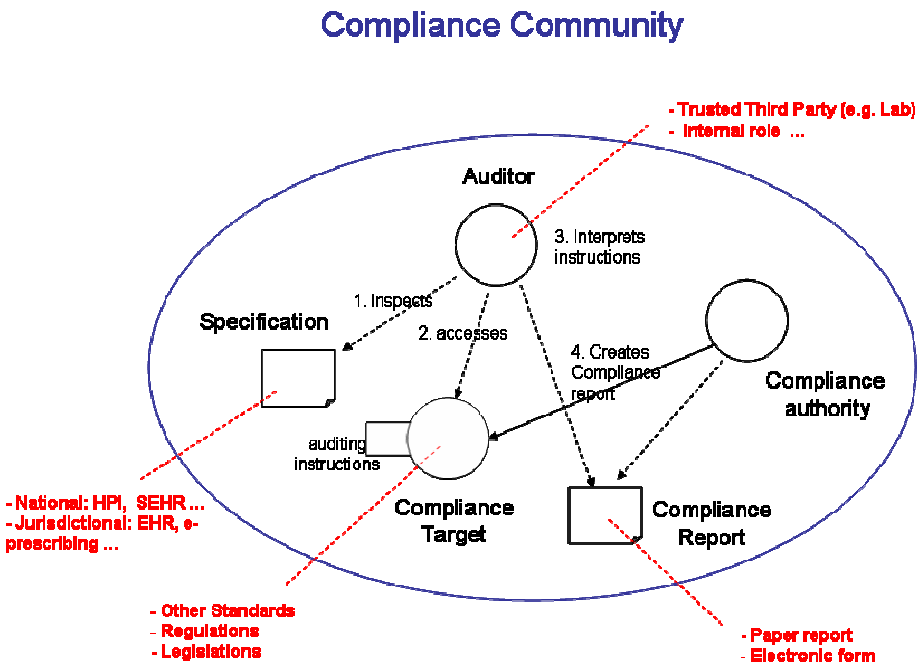

Figure 16: Compliance community

It is worthwhile noting that one special case of compliance requirement is pertinent to the NEHTA IF itself. There is, for example, a requirement that specifications within the NEHTA work program make use of the interoperability concepts and patterns of the IF. A measure of such compliance is described in [NEHTAIFv1.0] as a series of interoperability maturity levels.

6.6 Accreditation

6.6.1 Definition

Accreditation is a procedure by which an authoritative body gives formal recognition that an organisation or a person is competent to carry out specific tasks [CASCO]. The accreditation function is well established in the domain of testing laboratories. In this case, accreditation bodies, typically at a national level, e.g. National Association of Testing in Australia [NATA], can accredit testing labs, e.g. the Australian Health Messaging Laboratory [AHML], for their competency to undertake testing of products developed by other organisations, e.g. e-health vendors, to determine their conformance to standards and specifications.

In situations where products involve international trade, an international recognition for conformity testing and the associated accreditation bodies are increasingly becoming an important instrument in setting up and managing mutual recognition agreements (MRAs). In fact, recent trends in globalisation of world trade [WTO] place further emphasis on the international importance of accreditation bodies as a mechanism to address technical barriers to trade as part of the harmonisation of practices in standards, testing, certification and technical regulations [PC-NATA].

Note that often the testing labs also provide certificates for the products, which some consider to be a form of accreditation. The accreditation function is also well established to ensure competence of health professionals or health organisations, e.g. individual GPs, GP practices or hospitals. In Australia however, there is currently no accreditation for the vendors of e-health products.

6.6.2 Accreditation community

The objective of an accreditation community (see Figure 17) is to establish a clear framework for checking the competency of organisations or people in undertaking their tasks. The organisation can be any service provider including the providers that offer testing and certification services.

Key roles within this community include:

- Accreditation Target – this is a person or an organisation (i.e. the OIF party concept) whose competence needs to be determined for various tasks; these can be, for example, parties playing roles in conformance and compliance communities such as testers, certifiers and compliance auditors;
- Accreditor – follows a set of accreditation rules as described in a specification to assess the accreditation target and record the results of the assessment. Accreditation rules can specify different criteria for different levels of competence. For example a bronze, silver or gold maturity level criteria for an end user organisation regarding their capability to use the latest e-health products, or a similar ranking for a vendor of e-health products in their capability to deliver interworking and interoperable systems.

Note that as with the conformance community, the accreditation community may need to establish a control board role to facilitate dispute resolution. At this stage, such a role has not been included if is recognized that the need may arise. Suffice to say, this role can be filled by an appropriate legal entity.

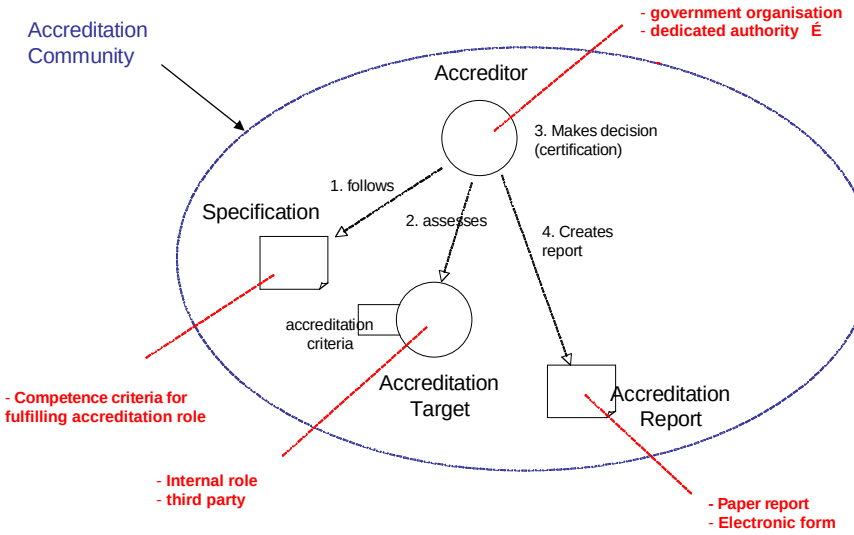

Figure 17: Accreditation community

6.7 Certification

6.7.1 Definition

Certification is a procedure by which a third party gives written assurance that a product, process or service fulfils a specification [CASCO]. Thus certification applies to each of the conformance, compliance and accreditation areas. For example, conformance certification by the AHML provides assurance that a vendor's HL7 messaging product satisfies some HL7 specifications, or HIPPA compliance certification provides assurance that a certain health organisation has implemented HIPAA privacy policies.

Note that the word 'certification' is sometimes used by independent third party organisations providing assurances that a certain organisation can be

'certified' because it has proven that the products, processes or services it provides are conformant with some specification, typically a standard. If used in this way, certification is a synonym for accreditation.

This document makes a strict distinction between assurances associated with a product (i.e. conformance) and assurances associated with an organisation's competency (i.e. accreditation), as also recommended by the ISO's Council Committee on Conformity Assessment [CASCO].

6.7.2 Certification process

The certifier role in the certification process can be played by a number of parties, e.g. in the case of conformance certification:

- Organisations or individuals can *self-assess* solutions based upon their own interpretation of the conformance criteria. This is a low cost, scalable solution to certification but provides little guarantee of a common certification outcome.
- A *national certification organisation* could be developed which supports all conformance statement types across organisational, information, and technical viewpoints. This is not a minor undertaking but does create the strongest guarantee of common conformance. The UK health reform work has followed this model by developing a large testing facility but their solution to e-health is based around common implementations, not common specifications.
- Several *organisations* already exist within Australia that provide conformance testing of e-health specifications. These include the Australia Healthcare Messaging Laboratory and organisations associated with Standards Australia. These organisations provide a low-cost entry point into conformance and distribute the load associated with such work.

It is also possible to migrate through alternative conformance approaches, beginning with self-certification and moving towards third-party certification.

6.8 Compliance criteria against the IF

The IF is a specification in its own right and the one with which many new e-health specifications, i.e. requirements, architectures and certification specifications should aim at complying with. This section lists high-level compliance criteria with the IF and also a number of detailed compliance points.

Note that the IF itself is compliant with the family of ISO RM-ODP standards [ODP-RM].

6.8.1 High-level compliance criteria

IF compliance refers to all of the following high-level compliance requirements:

- The adoption of the separation of concerns principle promoted by the IF in terms of technical, information and organisational perspectives of the system being specified.
- The support of interoperability methodology life-cycle, recognising the importance of each of the following stages, i.e. requirements, specification, certification and assessment (see Figure 18). In the case of conformance certification a specific implementation is to be tested against specification.
- The adoption of interoperability principles, concepts, goals and patterns, presented in this document.

6.8.2 Detailed compliance points

Further, the IF also identified the following more specific compliance points:

6.8.2.1 Community Model

The product documentation or specification should define a community model for stakeholders including policies, roles, actors, and artefacts.

6.8.2.2 Business Processes

The product documentation or specification must identify each business process associated with delivery of the product, service, or outcome. In addition, any assumptions about these processes must be documented.

6.8.2.3 IF and EA Analysis

The three Interoperability Framework perspectives (organisation, information, and technical) should be used to analyse interoperability support for the product or specification.

The NEHTA Enterprise Architecture Development Method and Principles must be followed. In particular, the product/specification documentation must be assessed against the Business, Information, Application, and Technical principles as well as follow the Enterprise Architecture Development Methodology.

6.8.2.4 Information Versioning

Mechanisms must be included to address versioning of information to support evolution of the product/specification. These versioning mechanisms must be explicitly documented in the interoperability assessment statement. A version history should maintain a graph of version split/merges including at least version identifier, source of information, and status.

6.8.2.5 Interaction Formats

The product/specification must document support for alternative forms of technical interaction including alternative information formats and connectivity protocols. There should be a clear distinction between syntactic representation of information (at least supported by a Web Services specification as described in 9) and the core business service specification (see 2) allowing for these alternative interaction approaches.

6.8.2.6 Information Quality

Information quality of information artefacts either generated by or stored within the product or service must be addressed. An information quality plan for creation and management of information should be created, including:

- metrics for the information quality characteristics such as those listed in section 4.4.4;
- assessment and if necessary accreditation mechanisms for information received from external sources,
- processes to identify and resolve information quality issues for both internal and external information sources.

6.8.2.7 Standards Focus

Standards compliance of the product or specification must be documented. These should include use of international, national, and other open standards where logically appropriate. Non-compliance with a relevant national or

international standard must be documented and reason given for such non-compliance.

A conformance statement should also be provided documenting assessment criteria for correct behaviour and interactions from other client or server systems. These criteria should cover each of the IF perspectives: organisation, information, and technical.

6.8.2.8 Architecture

Architectural assumptions of the solution or specification must be provided including

- separation into architectural tiers to support portal-based interfaces (presentation logic must be built upon a published functional service interface as described in 9) and
- alternative information sources.

This architecture guidance must set requirements for environments in which the product or solution will be instantiated.

6.8.2.9 Service Interface

Web service interface specifications must be defined for all external programmatic interaction points. These specifications should be produced shortly after the detailed functional specification as described in the NEHTA Enterprise Architecture Development Methodology.

The product or specification should support functional entry points through web service implementations and interact with external systems through web services. These interfaces must be augmented with assumptions about compatible business processes and interaction semantics (see 1).

6.8.2.10 Extensibility

A technical extensibility plan must be provided allowing for the incremental evolution of service interfaces, service endpoints, and other connectivity mechanisms. Service interface versioning should be supported. Release of new versions should be accompanied by appropriate documentation and support for vendors and jurisdictions to update their systems.

6.9 Summary

Figure 18 depicts positions the conformance, compliance and accreditation processes in relation to the life cycle of e-health projects. This life cycle involves requirements, specification, solution design and implementation phases. Note that these are the major phases in the interoperability methodology to be described in section 7.2.

Note that Figure 18 depicts another value assessment pattern, namely performance monitoring. In certain regulatory regimes performance monitoring is referred to as post-market monitoring, as for example done by the Therapeutic Goods Administration (TGA) in Australia [TGA].

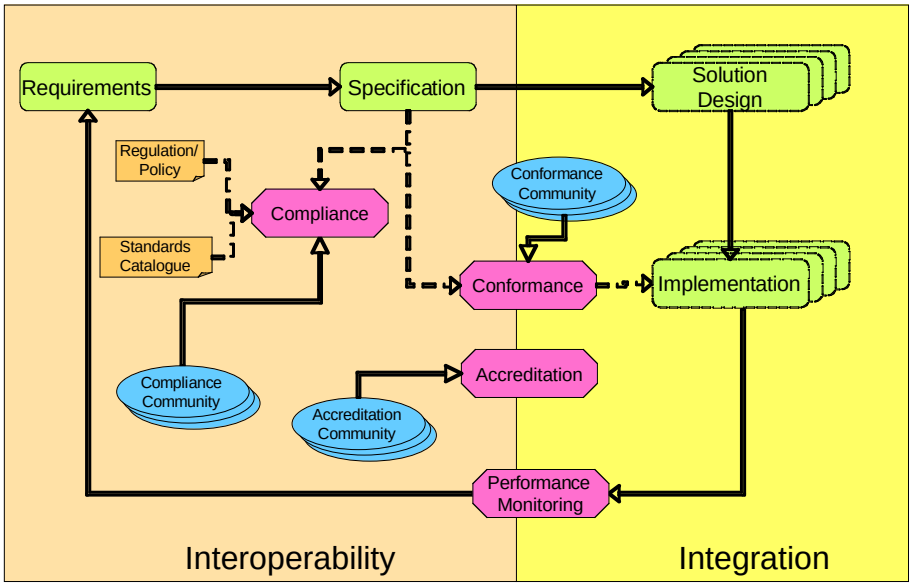

Figure 18: Role of Conformance and Compliance in Interoperability

The previous sections in this chapter suggest several milestones that are necessary to be reached in order to adopt a coherent approach to certification within Australian e-health, both within the community and organisational domains.

These milestones are:

- Explicit inclusion of conformance points in specifications, in particular those specifications that will form the basis for procurement processes
- The establishment of CCA governance in an organisational[22] context;
  - in case of compliance certification, this governance should ensure architectural alignment of different solution architectures in an organisation;
  - in case of conformance certification, the governance should facilitate either internal testing or external procurement activities
- The establishment of CCA governance in a community context;
  - in case of compliance certification, this would rely on the use of third-parties who would offer auditing services
  - in case of conformance certification, this needs the establishment of policies that cover the roles of testers, certifiers and accreditors, at the national level
- The establishment of a legal framework that supports the strategic and operational aspects of the governance above and ensures longevity and combination of market and regulatory forces to ensure the sustainability of a certification program.

[22] Section 8.4 provides description of interoperability domains, including organisational and community domains.

7 Foundations for Enterprise Architecture

The Interoperability Framework presented so far has emphasized a need for a *shared understanding* and the value of *common approaches* to implementing interoperability solutions. This is achieved through the adoption of a core set of interoperability concepts and an initial set of interoperability patterns respectively. In addition, the previous section has highlighted the role of CCA certifications as a type of *interoperability governance*.

Both of these strategies have significance for downstream architecture developments, namely:

- The semantics of interoperability concepts can constitute foundations for modelling languages adopted by enterprise architecture frameworks[23];
- The interoperability patterns can provide a base for further developments of architecture, design and test patterns;
- CCA certification provides a form of governance of relevance for architecture deployment including procurement, implementation governance, and architecture change management.

This section explains the approach taken by NEHTA in using the IF as a basis for the establishment of an enterprise architecture framework to cover the development of national e-health infrastructure with which NEHTA is tasked.

This version of the IF provides further detail to the EA ideas presented in the IF1.0. In particular it provides

- The rationale for the use of the TOGAF framework [TOGAF] for the development of EA for national e-health infrastructure with which NEHTA was tasked;
- The description of key customisation decisions to the TOGAF's framework;
- Further detail about the use of the SOA architecture style.

The section begins by outlining the high-level relationship between the IF and different enterprise architectures in Australian e-health (existing or future). This is followed by the description of a methodology to be used to guide the development of interoperable e-health systems, referred to as the IF methodology. This methodology sets the scene for an enterprise architecture methodology adopted by NEHTA, which is presented next. Note that this EA methodology is to be applied to all architecture efforts in which NEHTA is involved. This is to ensure enterprise alignment, and consistency between the architectural components of the national e-health infrastructure, for which NEHTA currently has responsibility.

7.1 IF and E-health Enterprise Architectures

The Interoperability Framework defines a language of concepts and patterns across three perspectives that enable cross-enterprise architecture cohesion. Each jurisdiction has or is likely to adopt an Enterprise Architecture Framework (EAF) that will lead to different enterprise architecture and toolset choices. As Figure 19 depicts, the IF works across this diversity of approaches to align conversations through the organisational, information, and technical perspectives. It is through this shared understanding and the adoption of common interoperability concepts and patterns between the IF and individual EAFs that this conversation can be most effective.

[23] Note that many such frameworks are agnostic to the choice of a modeling language.

NEHTA has established its own EAF to use in its creation of interoperable e-health infrastructure services for Australia. This EAF is used to guide all architectural developments of NEHTA's initiatives, namely the respective *solution architectures*. The aim is that through the adoption of the agreed set of architecture principles of the EAF, each solution architecture contributes to the emerging enterprise architecture for national e-health infrastructure. This approach ensures an iterative and incremental development of enterprise architecture, reflecting the responsibilities with which NEHTA has been tasked. Figure 19 depicts the co-existence of State and Territory, Federal, private sector, and NEHTA approaches to enterprise architectures (EA) and highlights the degree to which all contribute to a national e-health environment.

Note that the EAF adopted by NEHTA provides a coherent architecture framework for NEHTA services and is not a replacement for jurisdictional enterprise architectures. It provides a foundation for interoperability across the NEHTA services and may be reflected on by jurisdictions as being a potential approach to their own enterprise architecture issues.

It should be also noted that the IF is not a replacement for EAFs, but instead creates cohesion between the different EAFs through the aforementioned concept and patterns.

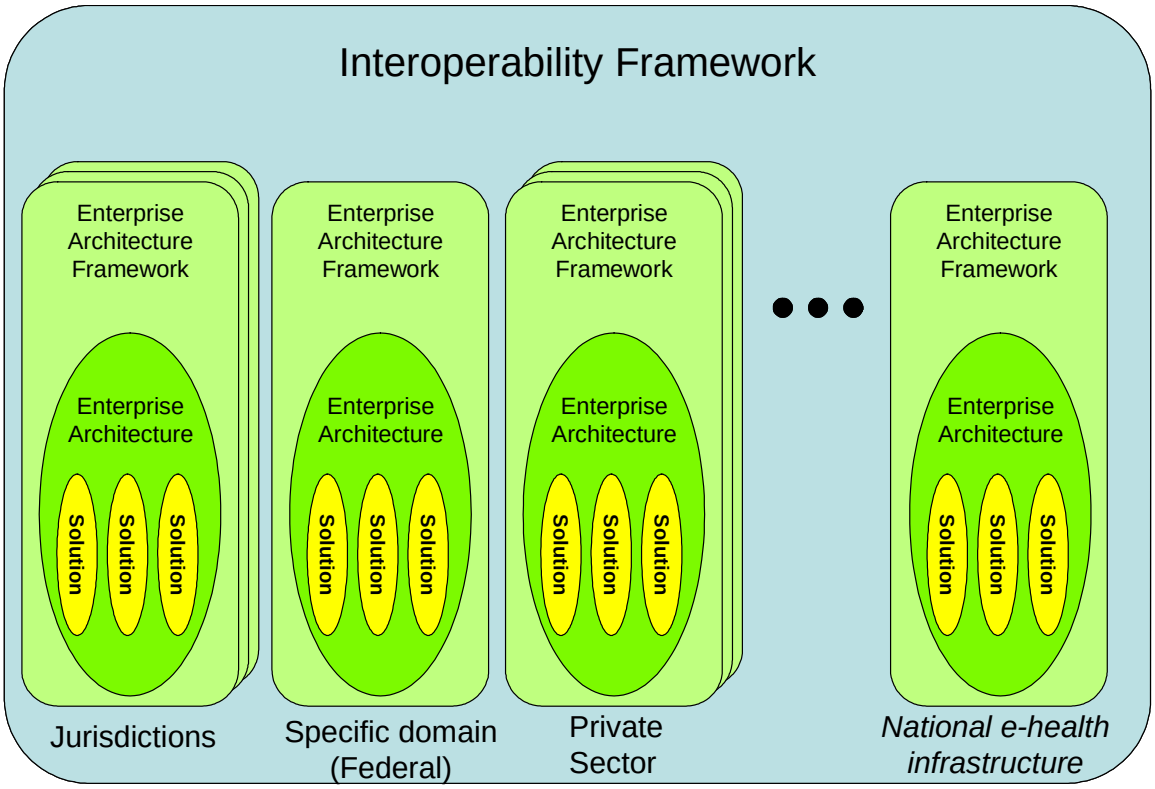

Figure 19: The Interoperability Framework as a family of enterprise architectures

It is expected that new contributors to the national e-health community will emerge and others will leave. Each will follow their own EAF approach but by mapping to the IF concepts and patterns, they equip themselves for future interoperability and subsequent integration.

7.2 Interoperability framework methodology

The Interoperability Framework requires a consistent high-level methodology to guide the initial phases of the solution delivery process, ensuring that future interoperability is achieved. This is not a replacement for an EAF methodology but should instead be viewed as a compliance requirement for an EAF methodology. This section positions the IF methodology and outlines its requirements.

Technical outputs that define or create an ICT capability are required to follow a standard IF methodology including requirements analysis, architectural specification, and compliance/conformance identification phases before choosing specific solution design, implementation delivery, and value assessment options (see Figure 18). Each phase comprises concepts and patterns from the three perspectives: organisational, information, and technical.

- *Requirements* capture and analysis is used to scope a business problem and (as Figure 20 depicts) the majority of requirements are going to be expressed in terms of organisational concepts and patterns. For example, the identification of key communities, statements of their objectives, and identification of the constituent business processes, roles and policies. In addition, the key information components supporting the organisational requirements will need to be identified, along with the key IIF patterns. There may also be technical requirements such as the use of SOA technical aspects.
- An *Architectural Specification* will describe the contribution a deliverable makes and relationships it requires to other technical system components. Depending on the system being described, architecture specifications will consist of varying degrees of organisational, information and technical content. Each of these specifications will be written in sufficient detail for the subsequent implementation phase. For example, an organisational specification will include a more detailed description of business processes than what is identified at the requirements phase. The architecture specification will also include a detailed information model and technical architecture. The technical architecture must be independent of technology and provider choice and present an architectural foundation based upon service principles including provision of reusable business services and separation of interface from implementation.

  A Service Relationship Statement must describe the service interfaces that are provided to other NEHTA services and those service interfaces that are required by the deliverables. The required service interfaces will also be part of the Compliance Statement.
- A *Compliance Statement* detailing all NEHTA, national, and international standards/specifications that are being utilised by the deliverables. This includes both those used within the deliverable and those with which the deliverables interoperate. It is strongly advised that all efforts be undertaken to be compliant with obviously relevant Australian Standards where possible and if not, a non-compliance statement should be provided.
- A *Conformance Specification* accompanying the Architectural Specification will identify a set of conformance points enabling certification of implementations against the Architectural Specification.

Compliance with the NEHTA IF methodology requires adoption of the concepts and patterns associated with the three interoperability perspectives as well as delivery of a set of documents detailing adherence to the IF methodology requirements.

The IF methodology is a high-level development methodology that reflects the transitionary and evolutionary spirit of NEHTA's contribution to the long-term interoperability of Australian e-health. The IF methodology has been developed to ensure vendor and technology independence, open standards compatibility, and the sustainable delivery of architecture specifications and subsequent IT system implementations.

The main aims of the IF methodology are to provide:

- a systematic and consistent way of delivering specifications based on a set of requirements;

- a disciplined and unambiguous approach in expressing compliance and conformance criteria (as described in section 6);
- an iterative and incremental way of developing specifications, according to a pre-defined project plan; and
- agility in terms of dynamic responses to external triggers including value assessment approaches.

In a similar way, as the IF represents a higher level of abstraction than EA frameworks so the IF methodology represents a 'higher-level' methodology than many EA methodologies.

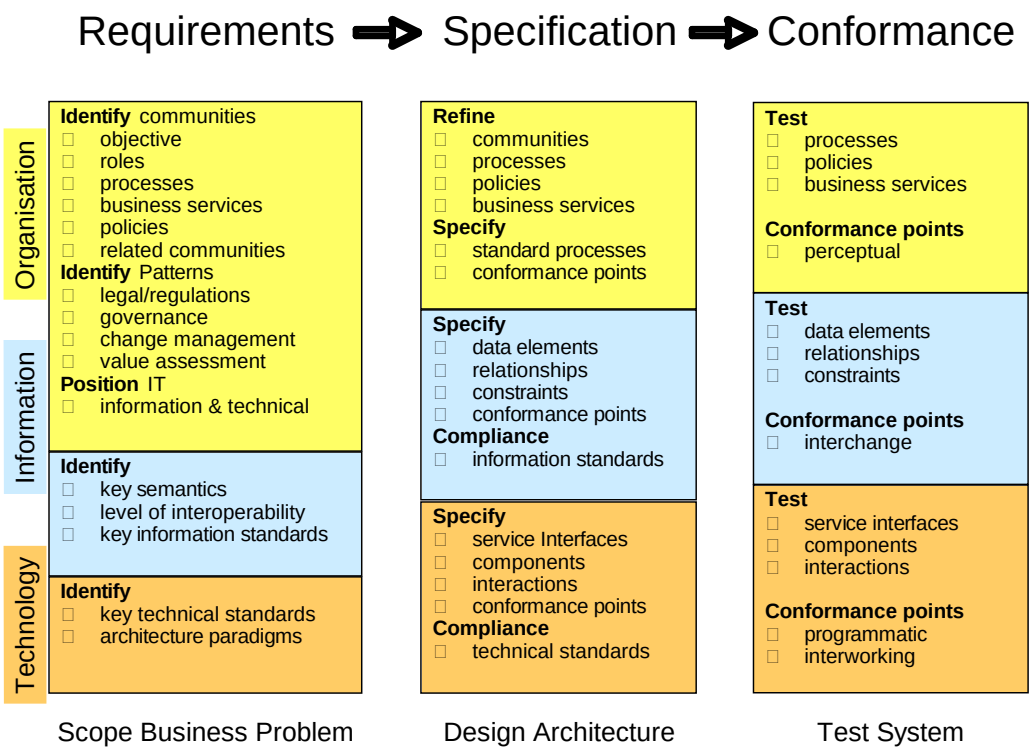

Figure 20: NEHTA standard IF methodology for requirements, specification and conformance

Note that the IF methodology also includes a value assessment phase (not shown in Figure 20). This phase is the key phase in providing a business justification for a solution before the development process starts. A post-release assessment determines the value of the system in use and possibly identifies points of possible incremental improvement.

7.3 Enterprise Architecture methodology of NEHTA

The purpose of this section is to provide an overview of the approach taken by NEHTA in establishing and developing an EAF to govern the development and implementation of that part of the e-health infrastructure with which it was tasked. This is referred to as an EA for national e-health infrastructure hereafter. The section also provides an outline of major architecture decisions made so far.

7.3.1 Adoption of the TOGAF standard

NEHTA has chosen to use the TOGAF enterprise architecture framework [TOGAF] to develop an EA for the national e-health infrastructure.

TOGAF specifies an architecture development method (ADM) to guide this development. The ADM defines an incremental, iterative approach to defining the EA, as shown in Figure 21.

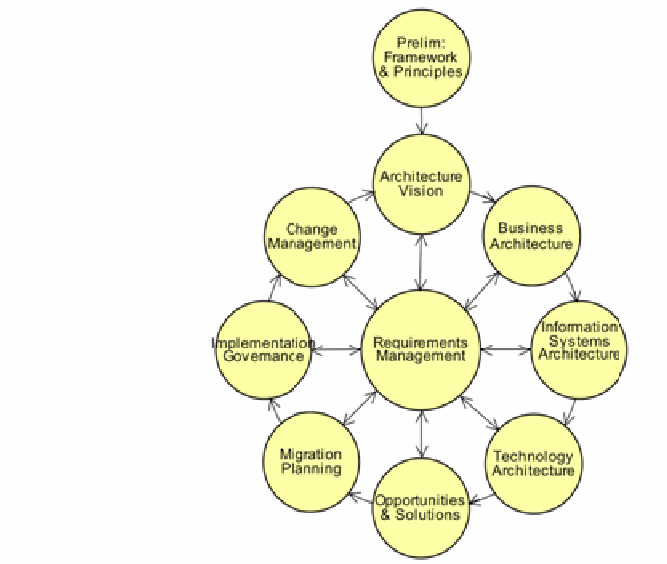

Figure 21: TOGAF's ADM

There are four types of architecture that are commonly accepted as subsets of an overall enterprise architecture, all of which TOGAF is designed to support [TOGAF]:

- A Business Architecture - which defines the business strategy, governance, organisation, and key business processes.
- A Data Architecture - which describes the structure of an organisation's logical and physical data assets and data management resources.
- An Applications Architecture - which provides a blueprint for the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the organisation.
- A Technology Architecture – which describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc.

Figure 22 depicts how these different architecture phases of the ADM are linked to the three perspectives of the IF.

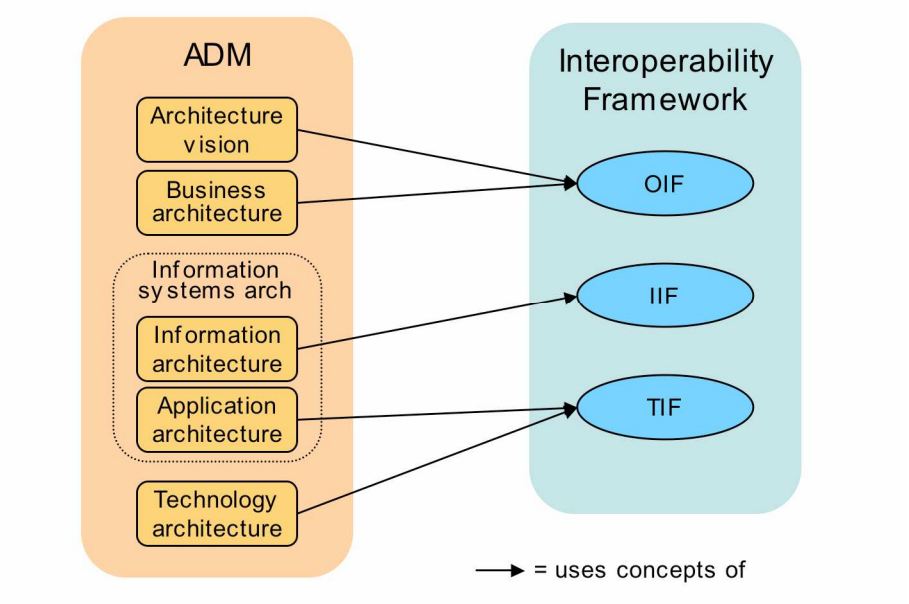

Figure 22: Relationships of ADM Phases to the IF

The ADM is also compliant with the IF methodology, with various phases corresponding to identified IF activities as depicted in Figure 23. Note that some activities identified in the IF methodology are out of scope for the ADM and are not shown.

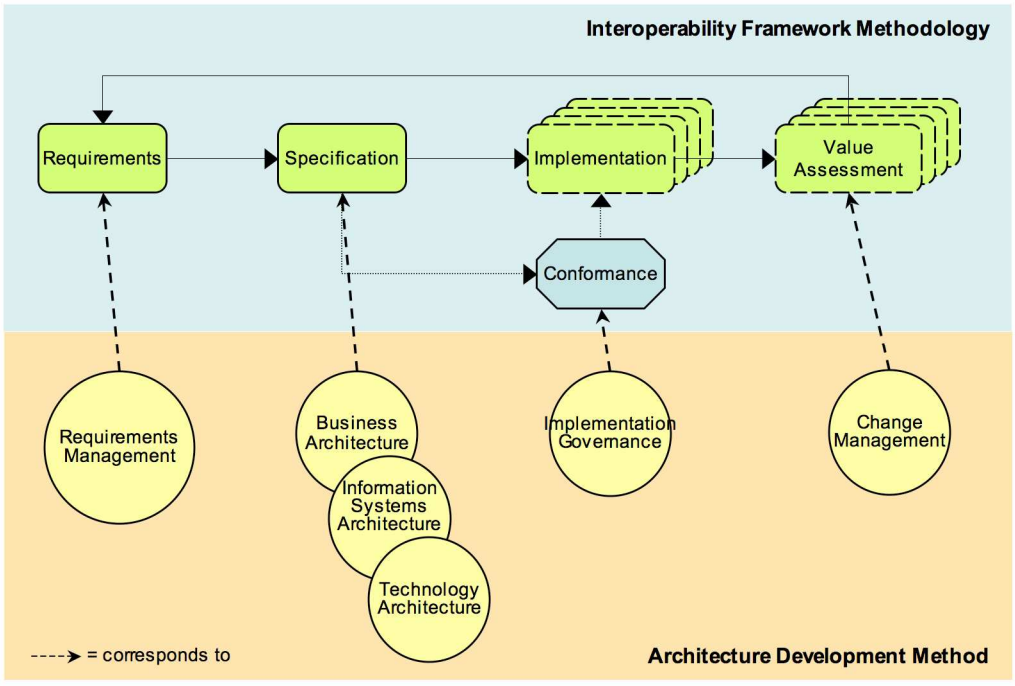

Figure 23: ADM Phases Related to IF Methodology

The choice to use the ADM as opposed to other EA frameworks was motivated by three facts:

- the ADM is *easily customisable* to reflect the needs of a specific organisation; in the case of NEHTA the customisation allows the use of the family of interoperability languages as modelling languages for each of the four architectures of the EA;

- the emphasis on a *continual process* supporting the development of 'just enough architecture' ; in the first iteration for example, the aim is to define a 'kernel' of EA which will grow according to the contributions from each of the solution architectures from NEHTA's initiatives. This approach ensures a common ownership model in which each initiative owns a fragment of the EA.
- the ADM encourages the establishment of *EA governance structures*, facilitating a coordinated approach in aligning different solution architectures of NEHTA's initiatives.

So, the NEHTA customised ADM provides a more concrete and directed methodology for use within NEHTA, while supporting compliance of NEHTA specifications with the IF.

The approach taken by NEHTA is thus to exploit the ADM to treat EA development as a continual process, while using the interoperability concepts as modelling languages for each type of architecture. Each initiative is expected to apply the ADM to populate the EA with the solution architecture of the initiative. Through applying the ADM and using the architecture principles (see the next section), the initiatives ensure the consistency of their architecture specifications across the national infrastructure.

As part of the preliminary phases, which included the customisation decisions above, the EA team has also:

- identified key architecture principles, which refine and extend the interoperability principles from in the previous sections;
- established an initial EA program consisting of a coordinated approach to developing, reviewing and publishing architecture specifications – this is part of the EA architecture governance.

The key outcomes of these activities are described in the following subsections. Initial versions of these deliverables were communicated to all Jurisdictions and it is anticipated that these deliverables will be made public in the second part of 2007.

The first step in developing an enterprise architecture using TOGAF is to specify a set of architectural principles, as outlined next.

7.3.2 Architecture principles

The TOGAF specification states:

> *Architecture principles define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise.*

Thus, the EA architectural principles should guide all subsequent decision-making related to the enterprise architecture and solution architectures governed by the EA.

TOGAF divides architectural principles into four categories:

- Business principles
- Information principles
- Application principles
- Technical principles

The following sub-sections list key principles for each of these distinct categories, with the TOGAF "Data principles" re-named "Information principles" to better reflect the terminology used in NEHTA. These principles are presented using the TOGAF format, i.e. the principle statement, rationale and implications.

Note that many principles were inspired by the interoperability principles, concepts and patterns presented in previous sections.

7.3.2.1 Business principles

- Primacy of Principles

  Statement: EA principles apply to those NEHTA initiatives specifying or building national e-health infrastructure components and services.

  Rationale: The only way to ensure consistent, high-quality service delivery for e-health infrastructure is if all initiatives abide by these principles.

  Implications:

  - Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the provision of a national e-health infrastructure.
  - New e-health infrastructure initiatives will not begin until they are examined for compliance with the principles.
  - A conflict with a principle will be resolved by changing the architecture specification of the initiative.

- Maximise Benefit to Healthcare

  Statement: decisions about e-health infrastructure components must always maximise the quality of care.

  Rationale: Where there is any conflict or uncertainty in making decisions about infrastructure specifications and services, the goal of providing better quality of care should take precedence.

  Implications:

  - The benefit to healthcare provided by an infrastructure specification or service must always be identified.
  - Decisions about technology should be driven by healthcare needs rather than technological or other concerns.
  - A simple solution that provides immediate benefit to healthcare organisations is preferred over a technologically better solution.
  - The Institute of Medicine quality of care principles [IOMQOC] should be applied to such decisions, that is, healthcare should be safe, effective, patient-centred, timely, efficient and equitable.

- Interoperability

  Statement: a core characteristic of all specifications is that they will support or enhance interoperability between healthcare organisations (covering all three interoperability perspectives).

  Rationale: A key reason for establishing a federal e-health infrastructure is to allow healthcare organisations to share information. Interoperability, starting at the enterprise level, is the basis for such sharing, and the core principles that govern the approach are captured in section 2.2.1.

  Implications:

  - Specifications should be openly available.
  - All specifications must be described in a manner that is compliant with the Interoperability Framework (IF). Compliance is more formally defined in section 6.5, but in this context, it means that the specification is defined in terms of the IF concepts, or a correspondence with IF concepts is explicitly defined.

  - Open and widely supported standards are a key element in achieving interoperability. They should be used as wherever possible.
  - Business-level interoperability is enabled by clearly identifying the community in which a specification or service is used, and how that community will use the service or specification to achieve better healthcare.

- The Business is e-Health Infrastructure

  Statement: The success of the national e-health infrastructure is measured by the quality and utility of services and specifications that are provided to healthcare organisations.

  Rationale: The role of the national e-health infrastructure is to support healthcare organisations in the provision of better healthcare services through e-health services and specifications. In effect, healthcare organisations are the customers and must be respected for the infrastructure is to be successful.

  Implications:

  - The infrastructure is not providing healthcare services. It is providing e-health infrastructure and shared services to those who provide healthcare services. The infrastructure should not dictate how they provide healthcare.
  - Services and specifications must be accessible to healthcare organisations: the infrastructure should not use technology or approaches that are technically or organisationally infeasible for them.
  - The infrastructure does not control the healthcare organisations. A co-operative, community-minded approach is much more likely to succeed than an autocratic approach.
  - The responsibility of the infrastructure stops at the organisational boundaries of the healthcare organisations. Initiatives should focus on scenarios that exist fully or partially outside the organisational boundaries of healthcare organisations in formulating requirements.

- Service-oriented Approach

  Statement: a service-oriented approach to the development of specifications and services will be applied.

  Rationale: A service-oriented approach requires that specifications and services provided by NEHTA provide an identifiable, relevant and cost-effective service to businesses using the infrastructure. The business-level service definition becomes the point of alignment between business, information and technical perspectives.

  Implications:

  - The business-level relevance and benefit associated with services must be identified.
  - Service usage is captured in process definitions that specify the interaction between service providers and service consumers. Processes might be as simple as request/reply or even a one-way message but can also be considerably more complex.
  - The business-level responsibilities of both service providers and service consumers must be identified in a process.
  - Processes provide the basis for agreement between service providers and service consumers, and as such, should reflect the

concerns of all parties involved in an instance of service usage. These concerns should be reflected in the services.

  - Services identify information (data) associated with service provision and use. In a service-oriented approach, an information model must be associated with business services using that model to identify the benefit to the business. Information models should not be specified without the context of one or more services.

- Compliance with Policy

  Statement: the infrastructure exists in a federally regulated environment and must comply with all legislative and regulative policies.

  Rationale: To ensure compliance with federal and other policies, an awareness of applicable policy is a fundamental need at all points in the enterprise architecture. This must be reflected in all specifications.

  Implications:

  - Applicable policy should be explicitly identified for all specifications at the business level in the enterprise architecture.
  - Policies should be specified in terms of the IF concepts of obligation, permission and prohibition and scoped by the community or communities that define them.
  - A separation between policy and mechanism should be maintained where possible: solutions should provide mechanisms to implement policy or demonstrate compliance with policy without hard-wiring the policies themselves. Policy specifications should be maintained separately from the business service.
  - Policy encompasses privacy and other requirements that are often dealt with through security mechanisms. This business-level principle still applies to those mechanisms.

- Information Rights

  Statement: information shared by healthcare providers has associated rights attributed to members of the healthcare community and these rights must be respected.

  Rationale: The national e-Health infrastructure is providing services for sharing health information and in most cases this information has associated rights, typically defined by the owner or via legislation. Rights to information must be considered in all use of the information to ensure that legal, social and ethical rights of parties are respected.

  Implications:

  - Ownership implies certain rights, but not necessarily complete control.
  - The ownership and rights associated with information should be explicitly recorded. Complex scenarios can arise and must be dealt with at the business level.
  - The IF provides an information rights pattern (see sections 3.4.1 and 4.4.1) that should be used as a guide for defining information rights.
  - Rights and usage constraints defined by the owner or implied by the community in which information is used should be captured and applied through appropriate policy constraints.
  - Information should not be modified without appropriate rights.

- Common Use Infrastructure

  Statement: development of components and services used across the national infrastructure is preferred over the development of similar or

duplicate components that are only used by a particular service or specification.

Rationale: Duplicative capability is expensive and undermines interoperability through inconsistency and ambiguity.

Implications:

- Initiatives that depend on components or services that conflict with or duplicate the existing infrastructure must change over to the national infrastructure components. This will require establishment of and adherence to a policy requiring this.
- Initiatives will not be permitted to develop capabilities for internal use that are similar/duplicative of enterprise-wide capabilities.
- Initiatives should ensure that similar enterprise-wide capability does not exist before embarking on infrastructure development.

- A Pragmatic Approach

  Statement: stating that solutions must be developed using a pragmatic approach that favours feasibility over architectural purity.

  Rationale: The e-Health community requires cost-effective solutions that can be implemented in relatively short timeframes. This requires that decision-making considers pragmatic concerns associated with implementation, operations and workplace culture.

  Implications:

  - Replacing existing systems is expensive, particularly in operational and training costs. Solutions should complement rather than replace existing systems.
  - Adoption of new approaches typically requires cultural change, which is best approached in small steps. Incremental improvements are thus preferred.
  - Consolidation of information currently held in disparate, autonomous repositories, while technically pure, is politically and culturally offensive to those who control those existing repositories. Approaches that retain existing control structures, for example through federated architectures, are considerably more pragmatic.

7.3.2.2 Information Principles

- Service-oriented Approach

  Statement: Services are the fundamental mechanism for sharing information.

  Rationale: The national infrastructure has adopted a service-oriented architecture to ensure alignment between business, information and technical concerns. To reflect this choice, sharing of and access to information must occur in the context of a service.

  Implications:

  - Published information models should be defined in terms of the information components that are passed during service usage. Note that the exception to this is where the information being shared is a schema itself (e.g. the archetype library). In these cases, there is an implicit expectation that these schemas will be subsequently used in service provision.
  - Publication and use of stand-alone database schemas for interoperability or integration is inappropriate.

  - Information quality control must be defined in terms of service constraints and explicit information quality processes associated with service usage.
  - Mechanisms for establishing visible relationships between information components should also be visible in service specifications. In other words, the fact the two or more services share a data source should be explicit in the service specifications if relationships realised by the sharing are visible in the information model.

- Terminology and Data Definitions

  Statement: a common understanding of concepts embodied in terminologies and data definitions is key to interoperability.

  Rationale: Interoperability is fundamentally enabled by the ability to communicate. Terminologies and data definitions capture the meaning and structure of shared information and thus must be shared and accepted in the community where they are used.

  Implications:

  - All services must identify or specify the terminology and/or data definitions associated with the information provided or received through the service.
  - Terminologies and data definitions must be openly published.
  - The IF concepts should be used as the basis for creating terminologies and data definitions.
  - The likely users of a service should be consulted in establishing terminologies and data definitions for a service. Or alternatively, an open standard that is widely recognised by the community should be used.

- Information Quality

  Statement: information quality is established through quality assurance processes.

  Rationale: An assessment of information quality is essential in providing accurate information for use by healthcare professionals. In an environment where there are many and varied sources of information, the quality of information generated by a given source is difficult to guarantee. Information quality must therefore be assessed by explicitly identified quality audit processes, with appropriate remedial action taken if required.

  Implications:

  - Information quality cannot be assumed.
  - Services having particular information quality requirements must engage in or identify processes to ensure that quality.
  - Remedial mechanisms for handling poor quality data should be defined, keeping in mind that information rights can limit or remove the ability of receivers to modify data. In general, the information will need to be returned to the source with appropriate annotation of quality problems, or the poor quality information will be flagged or quarantined to minimise its impact.

- Time, Space and Versions

  Statement: in a community of autonomous organisations, the time and place of creation of information components suggests versioning and are fundamental attributes of the component.

Rationale: Assessing the currency and veracity of an information component is critical in the provision of appropriate healthcare. The time and place of creation are required for that assessment, effectively defining the versioning and of information. A historical perspective of changes to a modelled information concept also has considerable value in this assessment.

The sharing of information across autonomous organisations implies that once shared, an information component cannot be destroyed or removed. The explicit modelling of time and space dimensions also provides a basis for handling this aspect of shared information.

Implications:

- Information components should always identify the time and place of creation of the information.
- An update to a modelled information concept is a new information component with a distinct time and place of creation, or in other words, a new version. Services providing sharing of or access to information might choose to keep only the most recent or most accurate version, but must acknowledge the existence of preceding versions. Maintaining an explicit and accessible version history representing changes to a modelled concept is preferred.
- The version history of an information component might contain 'forks' when independent updates are applied at different locations. The time and place attributes should be sufficient to identify these situations.
- Where appropriate, services should provide mechanisms to establish the currency of previously published information (e.g. time or version stamp comparisons).

7.3.2.3 Application Principles

- Service-oriented Approach

  Statement: services are the fundamental concept for specification of possible interactions with a party.

  Rationale: The national infrastructure has adopted a service-oriented architecture to ensure alignment between business, information and technical concerns. To reflect this choice, any interaction must occur through a service. Services are intended to capture re-usable elements of business functionality.

  Implications:

  - Any interaction with a party must occur through a defined service.
  - Any application-level service must contribute to the realization of a business-level service.
  - Service composition is achieved through process definitions

- Processes and Services

  Statement: processes are the fundamental mechanism for describing service composition and instances of service usage.

  Rationale: Services are intended to capture re-usable elements of business functionality that are largely independent of business processes. Service composition and distinct usage scenarios are formalised through process definitions.

  Implications:

  - Service composition is defined through process definitions.

  - A process should be defined for any service usage scenario. Common patterns of usage can be identified and re-used (for example, request/reply).
  - A service specification alone does not define service usage. The specification might, however, require or imply specific steps in processes defining service usage.

- Policy Compliance and Processes

  Statement: compliance with policy is ensured by processes.

  Rationale: Policies capture the constraints imposed by the regulatory environment in which processes (service usage) occur. Thus, processes must ensure that policy constraints are satisfied.

  Implications:

  - Processes can use both active and passive approaches in ensuring compliance: An active approach means that the process fails or refuses to continue if a policy is breached. A passive approach means that the process or an associated compliance monitor checks for policy compliance after service usage has occurred (i.e. auditing or business activity monitoring), reporting breaches to some authority for remedial action.
  - Providers and consumers of services might be required to provide additional functionality to support the process in establishing compliance, for example, access to audit trail information or alerts for policy-related events.
  - A combination of active and passive approaches is typically most effective and efficient.

- Loose Coupling

  Statement: processes and services must allow for loose coupling and sporadic disconnection of parties.

  Rationale: As discussed previously in 3, autonomous participants in processes are not always connected or might have limited connectivity. Processes and services should allow for disconnected operation and minimal dependence on the availability of a connection. For maximum robustness and scalability, loose coupling should be considered the rule rather than the exception.

  Implications:

  - Coupling is most invasive for long-running activities. Stateless approaches, where each service invocation is self-contained and requires minimal communication context, promote loose coupling.
  - Activities primarily aimed at recording observations or developing information content should be self-contained and able to be completed when disconnected.
  - Web-based applications that rely on state stored on a remote server should be reserved for activities having a short duration and those that are not critical to the local operations of a health-care organisation.
  - Transactional or store-and-forward messaging can be used effectively to support loose coupling.

7.3.2.4 Technical Principles

- Service-oriented Approach

  Statement: technology choices and solutions must implement a service-oriented approach.

Rationale: The national infrastructure has adopted a service-oriented architecture to ensure alignment between business, information and technical concerns. To reflect this choice, implementation and deployment of technology solutions should be directly linked to the provision of business-level services.

Implications:

- Technology should not be deployed unless it is required for the provision of one or more identifiable business services.
- Technology that defines its interaction with external parties via a set of openly published service specifications is preferred.
- Technology that does not openly publish service specifications for its external interactions should be avoided.

- Policy-driven Solutions

  Statement: technology choices and solutions should clearly identify policy management mechanisms and allow the externalisation of policy definitions.

  Rationale: The IF highlights the need for clearly identified policy definitions in the e-Health community. Other architectural principles require the separation of policy from mechanism. Technology choices should reflect these influences.

  Implications:

  - Technology and solutions that support the explicit externalisation of policy are preferred.
  - Technology and solutions that embed or imply policy should be avoided.

- Observance of Standards

  Statement: all solutions should apply standards in accordance with the national e-health standards development management framework [STANDARDS-M].

  Rationale: Application of appropriate standards is a key element of interoperability. NEHTA has published a management framework for standards and this should serve as the basis for applying standards to solutions developed for the national infrastructure.

  Implications:

  - Consensus standards are preferred.
  - Choices should comply with the WTO Code of Good Practice for the Preparation, Adoption and Application of Standards [WTOCODE]. In particular, local standards have should be preferred when they exist.

- Requirements-Based Change

  Statement: changes to technology should be made only in response to business needs.

  Rationale: This principle will foster an atmosphere where the national e-Health infrastructure changes in response to the needs of the business, rather than having the business change in response to information technology changes. This is to ensure that the business purpose of the infrastructure - the sharing of health information - is the basis for any proposed change. Unintended effects on business due to information technology changes will be minimized. A change in technology may provide an opportunity to improve the business process and hence, change business needs.

Implications:

- Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.
- Technical improvements or system development should not be funded unless a documented business need exists.
- Change and requirements management processes conforming to this principle will be developed and implemented.
- This principle may bump up against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. Purpose of this principle is to keep us focused on business, not technology, needs--responsive change is also a business need.

- Contained Operational Cost and Complexity

  Statement: solutions must have well-defined operational cost and complexity.

  Rationale: Solutions in the health sector are often more expensive to operate than to develop. The operational cost and complexity of a solution must be identified and contained to ensure ongoing operation of the solution is feasible. Deployment, migration and cut-over processes are particularly sensitive to complexity, delays and other operational issues.

  Implications:

  - Operational procedures and their likely cost must be identified early in the process of selecting and/or developing a solution.
  - The deployment, migration and/or cut-over strategy for any solution must be identified in assessing the operational cost and complexity.
  - Where possible, the approval of the organisation(s) responsible for deploying and operating the solution should be obtained before proceeding with a selected technology or approach.

- Responsive Change Management

  Statement: changes to the national e-Health infrastructure are implemented in a timely manner.

  Rationale: If people are to be expected to work with the national e-Health infrastructure, that infrastructure must be responsive to their needs.

  Implications:

  - Processes for managing and implementing change should not create delays.
  - A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.
  - If we are going to make changes, we must keep the architecture updated.
  - Adopting this principle might require additional resources.
  - This principle will sometimes conflict with other principles (e.g., Requirements-based change).

- Controlled Technical Diversity

  Statement: technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between distinct technologies.

  Rationale: There is a real, non-trivial cost of infrastructure required to support alternative technologies. There are further infrastructure costs incurred to keep these technologies interconnected and maintained. Limiting the number of supported technologies will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

  Implications:

  - Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
  - Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
  - This principle is not intended to prevent the introduction of new technology. New technologies will be introduced when compatibility with the current infrastructure, improvement in operational efficiency, or a requirement for the new capability has been demonstrated.

- Security Policy and Risk Assessment

  Statement: security policy is a business decision trading off risks against benefits and should not be driven by technology.

  Rationale: Security decisions can have a significant effect on the operations and effectiveness of solutions. A decision based on technology can often impose operational constraints that make a solution unworkable or fail to address business risks not covered by the technology. Security policy for any specification must therefore be based on identifiable business risks and benefits.

  Implications:

  - Security policy and the risk assessment justifying the policy must be specified in the business architecture.
  - Technology decisions are limited to implementation of policy, and should not apply technology because it is more secure unless dictated by policy.
  - Security policy implementation might not require a technical solution, for example, privacy policy might be enforced through auditing and subsequent dismissal of staff found to have breached the policy, or electronic intrusion prevention might require staff to shut down their desktop machines when leaving work each day.
  - The security mechanism and security policy specifications should be maintained separately.

7.3.3 Service-oriented Architecture

The NEHTA has adopted a SOA architecture style to address a number of interoperability challenges in the national e-health infrastructure. In order to

deal with the lack of explicit support for the SOA style in the TOGAF 8.1, a further customisation of the ADM was needed.

A service-oriented approach ties business requirements to business services and processes, with these two concepts (service and process) providing the abstraction that links application and information architectures. The service and process abstractions are carried through to these application and information architectures to support the service-oriented approach.

7.3.3.1 NEHTA initiatives

Further details of the service oriented approach taken by NEHTA are provided next[24].

NEHTA will make a significant contribution towards transitioning e-health to an interoperable future where new solutions will be created for problems we may not have yet recognised. Some service solutions will be generated in local communities, others by jurisdictions, and some will be provided nationally. These parts must all co-exist and interoperate without disenfranchising parties contributing to a national e-health future.

Services will be provided in different forms by different parts of the community as changes occur in the understanding and ownership of e-health issues. For example, it is likely, and desirable, that local communities and jurisdictions work with new technology approaches that, over time, may manifest themselves as national approaches or services.

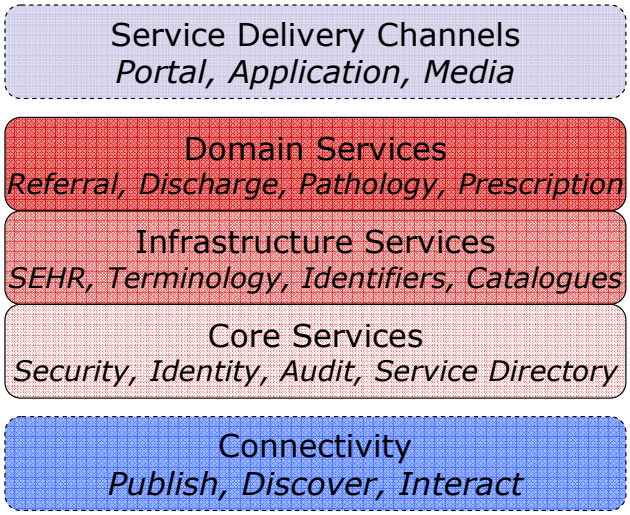

Figure 24: Layers of the NEHTA enterprise architecture

Distributed systems have taught us that a sedimentary effect occurs within infrastructure over time. What was once an application component becomes part of the infrastructure as it permeates the environment.

The NEHTA infrastructure describes a set of services and connectivity approaches required to deliver the technical capabilities of the NEHTA Enterprise Architecture. The components of the NEHTA infrastructure have been dissected into service delivery channels, shared services, foundation services, and connectivity mechanisms as summarised in Figure 24 and outlined below. This identifies the roles different infrastructure components play in supporting a variety of e-health outcomes.

- *Service delivery channels* provide the layer through which end users interact with systems. They range from shared portal technology to specific applications and media technologies such as DVD and written forms. Each channel carries ownership of some business logic but relies upon infrastructure components to deliver end user solutions.

[24] Note that much of this description fits the technical interoperability perspective.

- *Domain services* encompass services of relevance for specific health domains such as pathology, radiology, hospitals and general practice.
- An *infrastructure service* is used by one or more domain services for a common purpose. For example this might be access to a shared repository such as a medicine or national product catalogue, a national clinical terminology or identifier, or shared EHRs.
- *Core services* are a more basic element of the environment required for meaningful operation of infrastructure services and domain services. This includes mechanisms such as security, identity management, and service directory.
- *Connectivity* includes support for the publication, discovery, and interaction of services. Key to such connectivity are the standard protocols for connectivity.

Over time we would expect some change in status between different elements of this layering. In particular, the transition of shared services through to foundation services as parts of the infrastructure become more essential than optional. No governance or implementation ownership is presumed through these layers. In fact it is likely that multiple delivery alternatives will be employed across all layers as many parties deploy systems to meet the architectural requirements in regional, jurisdictional, and national communities.

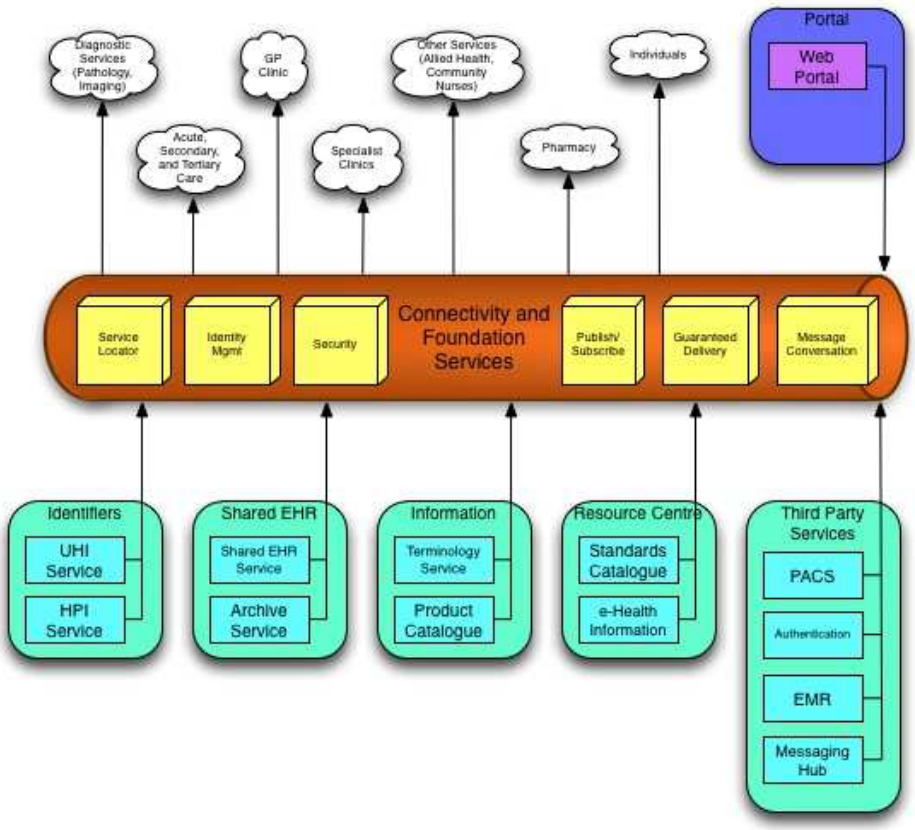

Figure 25: NEHTA initiative delivery within the NEHTA enterprise architecture

A high-level and service-based view of the EA adopted by NEHTA for the development of national e-health infrastructure is shown in Figure 25[25]. The figure depicts the broader e-health community working through the connectivity and foundation services (represented by the box framed by a dashed line) to access many of the shared resources within the NEHTA work

[25] This figure was inspired by a related architecture diagram from the Canadian Infoway project [Infoway]

program. NEHTA specifications determine how these services will interact but do not imply NEHTA ownership or operation of their implementation. Some, such as the connectivity environment have no single implementation but rather are the result of orchestrated implementation of a single specification by many parties. Other services such as a product directory may have a single national instance or may have multiple jurisdictional instances. Each, however, will be conformant to a single national specification.

The SOA approach can deliver direct business value by making business drivers the conduit for technical outcomes rather than driving business outcomes from technical solutions. It uses the concept of a service interface as part of the service specification to separate an implementation from the agreement that service makes with those using that service.

Such service agreements are not only of relevance to the infrastructure but also form part of the relationship with clinical care systems.

Figure 26 on the following page describes the relationships between clinical care systems accessing shared national services, which in turn rely on foundation services. Each element in the picture requires a services specification whether it is the interface specification for user authentication or the interface to a GP clinic.

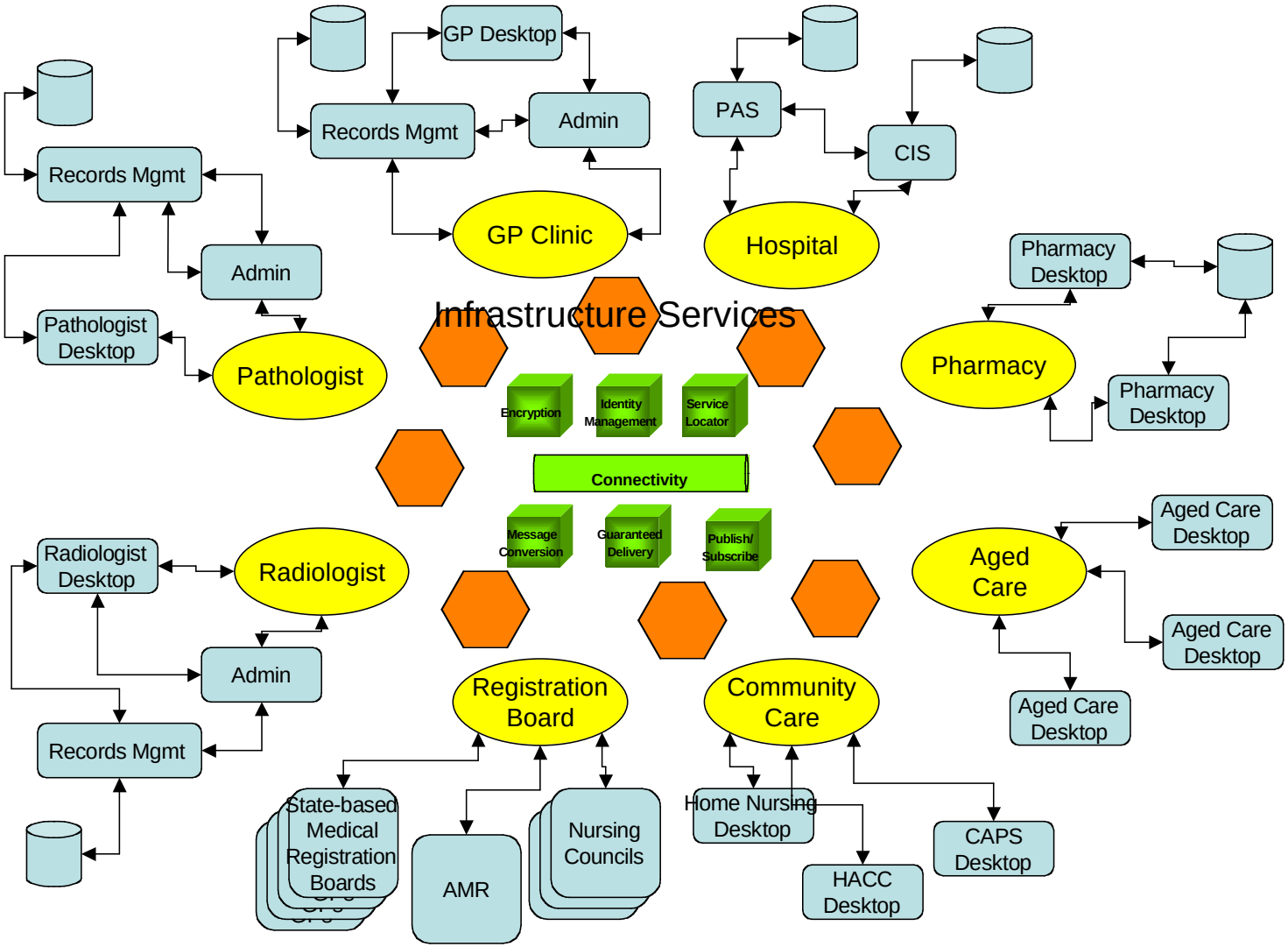

Figure 26: Service use from infrastructure to service delivery channel

Since services are the building block of SOA approaches, it is essential to agree upon a standard set of foundation service specifications as well as shared service specifications from which e-health solutions can be delivered. NEHTA is developing these service specifications as part of its deliverables. In addition, international efforts are underway to standardise service specifications through HL7 and the OMG. These efforts will bring together the vendor community with the various national e-health initiatives as well as aligning jurisdictional and community outcomes.

Even though the TIF describes multiple architectural patterns, foremost for the EA approach taken by NEHTA is an SOA-based approach. It is envisioned that NEHTA will also require adoption of an event-based model for asynchronous information delivery in future. As demonstrated needs arise and expertise increases, this will be added to the next versions of the EA for national e-health infrastructure.

7.3.3.2 Policy-driven

The ADM explicitly includes policy as a fundamental element in all stages of the process. This reflects the architectural principles relating to policy [PRINCIPLES] and ensures that initiatives adequately address the need for policy change and monitoring/compliance in a manner independent of the implementation approach.

7.3.3.3 NEHTA Alignment

NEHTA has a very active program of work specifying, and sometimes implementing, various aspects of the NEHTA Enterprise Architecture building blocks used to deliver an interoperable e-health environment. It is not only critical to deliver the right services into this environment but also to align the process of delivery to ensure a flexible and agile result is achieved.

NEHTA shall therefore ensure that:

- All initiatives undertaken by NEHTA are in compliance with the NEHTA EA and Interoperability Framework Methodology;
- Proposals for new services and components are considered in the context of the NEHTA EA; and
- NEHTA's architectural specifications are consistent with the Interoperability Framework and NEHTA EA.

7.4 Architecture deliverables

Each of the ADM phases has its own set of deliverables.

The table below provides a summary of how NEHTA deliverables can be associated with each phase of the ADM. Notice that the table also depicts how various components of the IF can be related to such deliverables.

The use of the OIF community concept and respective patterns can be used to capture business requirements. Iteratively, information and functional requirements can be expressed in terms of the respective IIF and TIF concepts.

Phase	Deliverables
Phase A: Architecture Vision	Community Goals, NEHTA Goals, Policies and Cost Drivers
	Existing and Target Business Scenarios (defines requirements)

Phase	Deliverables
	Conceptual Architecture (OIF)
	Business Case
	Statement of Work
Phase B: Business Architecture	Business Architecture (OIF)
	Initial Technical Requirements
	Gap Analysis
Phase C: Information Systems Architecture	Information Architecture (IIF)
	Application Architecture (TIF)
	Updated Technical Requirements
	Gap Analysis
Phase D: Technology Architecture	Technology Architecture
	Updated Technical Requirements
	Gap Analysis
Phase E: Opportunities and Solutions	Implementation and Migration Strategy
	Impact Analysis
Phase F: Migration Planning	Detailed Migration Plan
	Detailed Implementation Plan
	Impact Analysis
Phase G: Implementation Governance	Compiled requirements and technical architecture for projects
	Conformance and compliance criteria for projects
	Governance process definition for projects
Phase H: Change Management	Architecture Updates
	Request for New ADM Iteration
	Updates to Framework and Principles

Table 1: Summary of architecture deliverables

8 Interoperability guidelines

This section provides several guidelines that can be used by interoperability architects in the process of designing and analysing interoperability issues in e-health systems. These guidelines were identified in the course of undertaking two sets of activities since the publication of the IF1.0, namely:

- the development of the interoperability maturity model (which will be presented in Chapter 9);
- interoperability analysis of several e-health case studies.

The first set of guidelines highlights the need for organisations to define the key interoperability concerns of relevance for their e-health systems and to do this on a regular basis, say annually. This is done in terms of a selected set of interoperability goals that an organisation identifies. A number of such interoperability characteristics proposed by NEHTA is introduced in the next section.

The second set of guidelines describes approaches to linking interoperability goals and patterns. These in turn provide input into the third set of guidelines related to the analysis of interoperability solutions adopted (or to be adopted).

The final set of guidelines presented describes how different interaction boundaries determine the domain of interoperability.

8.1 Defining Interoperability Goals

Section 2.2.2 introduced a number of interoperability characteristics to facilitate the description of the complex notion of interoperability by breaking it into a number of constituent elements. These characteristics are defined in a way that they can be quantified, either applying subjective or objective measures. As a result, the interoperability characteristics can be treated as key interoperability goals whose realisation contributes to overall interoperability. Interoperability goals identify characteristics that have been put forward as common issues of concern. One specific use of interoperability goals is in the context of the interoperability maturity models but they have more general applicability as guidelines for assisting the analysis and design of interoperability targets.

Goals have been identified for each of the organisational, information and technical perspectives. In addition, common goals have been identified which are also to be applied to each perspective. The goals that will be presented below were identified through analysing interoperability in the national e-health community context, but they are also relevant to enterprise or local domains, including state and territory health enterprises (see section 8.4).

Although the current goals are comprehensive, it is anticipated that e-health organisations may wish to tailor these for their own use, or identify additional goals reflecting their own enterprise interoperability concerns. This should occur during the establishment of an interoperability maturity program.

Interoperability goals can be realised by adopting or reusing the interoperability concepts and patterns. Some patterns such as governance have a one-to-one correspondence to interoperability goals while others such as Service-Oriented Architecture support multiple interoperability goals.

8.1.1 Common goals

There are common interoperability goals that apply to each of the organisational, information and technical aspects of interoperability. Thus, the

following should be considered in concert with the interoperability goals presented in sections 8.1.2, 8.1.3 and 8.1.4.

The common interoperability goals identified by NEHTA are:

- *Reuse:* Leveraging previous solutions or knowledge, ensuring consistency between past and new solutions, and mitigating the risk of different interpretations, and the risk of duplicated solutions to the same problem or concept. Examples include the reuse of role descriptions (organisational perspective), reuse of standard clinical information concepts (information perspective) or reuse of system services supporting authentication, demographics management or user interfaces (technical perspective).
- *Evolution:* Treating change as an integral part of design including versioning and extensibility points.
- *Standards basis:* A special kind of reuse reflected in the adoption and implementation of nationally recognised and agreed open standards supporting a set of alternative, but standards-conformant implementation options.
- *Scope:* A clear delineation of system boundaries, i.e. what is part of the problem space and what is not. This then enables development of processes and technologies to interoperate across this boundary in well-defined ways.
- *Scalability:* Allowing for growth beyond initial capacity through identified mechanisms for capacity increase.
- *Configurability:* Support for elements of a specification or system that may change over time (e.g. enterprise or regulatory policies) as opposed to those more fixed foundational elements (e.g. well established healthcare processes and services).
- *Explicitness:* Ability to clearly isolate design artefacts (or implementation choices) representing specific concerns, to enable replacement, reuse, and evolution. Examples are the explicit differentiation of the content of e-health messages from their communication protocol structure; an explicit definition of technical services in a technical architecture (each of which implements a clearly identified piece of technical functionality); or an explicit expression of key business services (in a business architecture).

These common interoperability goals will have many interpretations across the interoperability perspectives described below. Their intent is to capture many fundamental ICT interoperability goals.

8.1.2 Organisational

The organisational interoperability goals identified by NEHTA are:

- *Business focus*: Clear description of a business problem, followed by a set of business requirements, and subsequent traceability to technical solutions (as opposed to a technically focused approach), allowing for possible later changes in business requirements.
- *Governance:* Separate governance for design, implementation, production and procurement processes for ensuring pro-active adherence to interoperability principles.
- *Overhead to change:* Recognition of processes and associated costs for solution de-provisioning. This including costs of integration points and other dependencies, so that it is possible to determine an optimal path for solution replacement, as well as costs associated with maintenance and commissioning.

NEHTA's Interoperability Framework highlighted the organisational issues that underpin interoperability. They are particularly critical in the multi-enterprise and cross-jurisdictional setting of the e-health community.

8.1.3 Information

The information interoperability goals identified by NEHTA are:

- *Data format vs. semantics:* A clear distinction between data representation (syntax) and model (semantics), allowing alternative data formats for implementation.
- *Meta-data:* Common definitions for the structure and description of information associated with data artefacts allowing for the context of information to be shared and commonly understood. For example this may include schemas defining data structures (XML Schema) or descriptions of author, creation date, and document version.
- *Ownership and rights:* The clear separation of permissions, rights and ownership of information to allow for the controlled and predictable creation, use and modification of information.
- *Common building blocks:* A special kind of reuse within the information perspective, supporting aggregation and association of data from different sources and encouraging shared use by different systems.

Clinical information specifications have always been a strength of e-health and their support for interoperability is enhanced through their strong reuse as well as independence from any technical implementations.

8.1.4 Technical

The technical interoperability goals identified by NEHTA are:

- *Interface specification:* Describing technical functionality independent of implementation, to enable change of technology options, while keeping the independence of the system boundary intact e.g. change in the underlying database or the platform implementing Web Services.
- *Functional decomposition:* Appropriate separation of solution components providing the building blocks for future evolution, aggregation, and reuse, through new compositions or abstractions.
- *Communication Protocol*: Independence of communication protocols from business logic allowing for support of new interaction paradigms, as they emerge, e.g. event oriented protocols.
- *n-tier architecture:* Explicit separation of user interface, business logic, and data stores, as well as identification of other possible tiers.
- *Technical policy separation:* Enabling independent specification of policy from solution interpretation (i.e. separation of policy from mechanism), so that, over time it is possible to change or use more sophisticated policy solutions for policy enforcement.

Technical issues are also often referred to as architectural goals in that they describe fundamental solution constraints that enable future interworking of independently developed work.

8.1.5 Discussion

The interoperability goals allow for future interoperability in a way that is both more predictable and cost-effective. Each application of these goals should map them into their unique context and highlight the use of specific interoperability standards, e.g. SNOMED-CT.

Table 2 below summarises the interoperability goals presented.

Goals	
Common	Reuse
	Evolution
	Standards basis
	Scope
	Scalability
	Configurability
	Explicit
Organisation	Business focus
	Governance
	Overhead to change
Information	Format and semantics
	Metadata
	Ownership and rights
	Common building blocks
Technical	Interface specification
	Functional decomposition
	Communication protocol
	N-tier architecture
	Technical policy separation

Table 2: Interoperability goals

Note that it is possible to distinguish two broad categories of interoperability goals.

Some goals simply specify requirements in terms of attributes of interoperability at certain point in time, such as requiring that a specification has explicitly identified service interfaces (to ensure various implementation choices) or requiring that a specification is compliant with privacy policies.

Other goals specify more complex effects requiring the establishment of certain procedures and processes, such as evolution, configurability, governance and low overhead to change. The implication is that some goals have one-to-one correspondence to interoperability patterns, such as for example governance.

8.2 Linking Concepts and Patterns to Goals

Each interoperability goal can be supported through the adoption of one or more interoperability concepts or reuse of appropriate interoperability patterns. This can be done either as part of e-health system design, or in the context of organisational practices established to support interoperability outcomes as part of an interoperability maturity program.

For example, the evolution goal can be supported by the SOA architecture pattern and through the explicit identification of patterns addressing enterprise polices, as shown in the figure below.

Note that the SOA pattern can support a number of other goals, including business focus and interface specification. Several examples of the mapping between concepts and goals are given in Figure 27.

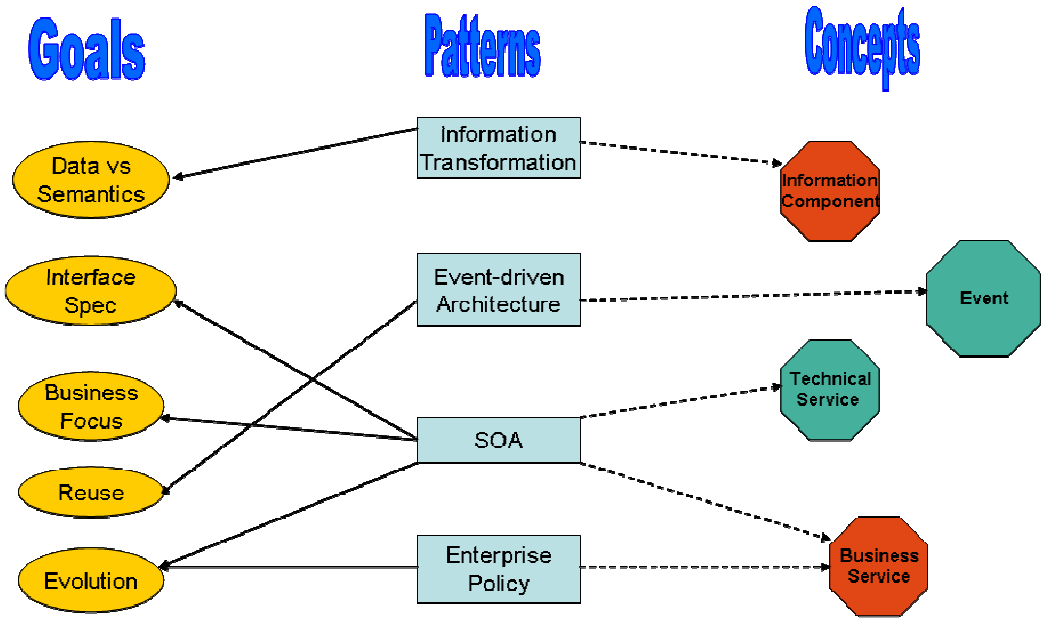

Figure 27: Linking patterns and goals

8.3 Interoperability analysis

The expression of interoperability in terms of interoperability goals, and the availability of existing interoperability concepts and patterns, can be considered as tools to facilitate various interoperability analysis activities. For example:

- interoperability assessment of existing e-health systems and projects
- the elicitation of interoperability requirements for implementing new interoperability solutions
- the design of interoperability maturity trajectories reflecting the benefits realisation priorities.

There are two approaches that can be taken, i.e. goal-oriented and pattern-oriented approaches.

8.3.1 Goals-oriented analysis

This analysis uses the interoperability goals identified in the previous section and determines to what extent an existing e-health system supports these goals.

The goals can be used to determine:

- interoperability attributes of specific e-health systems, e.g. how a GP system supports reusability, configuration or technical interface specification or
- organisational processes and practices established to support certain interoperability goals.

This goals-oriented approach has been adopted as part of the NEHTA Interoperability Maturity Modelling (IMM) specification.

The e-health system capabilities were considered as 'work products', while the organisational support for implementing interoperability solutions were considered as 'interoperability practices'. This is in line with the widely used CMMI model. Chapter 9 provides further insights into the IMM approach. For a complete description see the NEHTA IMM specification [IMM].

8.3.2 Pattern-oriented analysis

In the course of undertaking the interoperability assessment of several e-health projects using the analysis method above, it was found that this method provides a good in-depth analysis of project interoperability support. This is because it is based on a comprehensive set of interoperability goals.

In addition, the analysis has also identified the value of applying an alternative method that uses a number of interoperability patterns. An e-health system can be analysed in terms of whether it faces the problems for which the corresponding patterns are developed, e.g. whether there are situations in which standard business processes could be of use, whether meta-data is needed to support versioning, or whether there are situations which require design that is resilient to changes in policies and the way the policies are implemented.

This pattern-based assessment uses the IF interoperability patterns as a starting point and then identifies the interoperability goals that are realised through the use of such patterns.

Note that goal-driven and pattern-driven assessment analyses can identify different solution traits and therefore their combination contributes to a more comprehensive analysis of interoperability support within a work product.

Figure 28 below illustrates two possible analysis approaches, reflecting the linkages between patterns and goals. Both of these approaches can be used to assess a work product and thus they provide different, but related analysis methods. The figure also depicts the fact that interoperability patterns are used to realise interoperability goals.

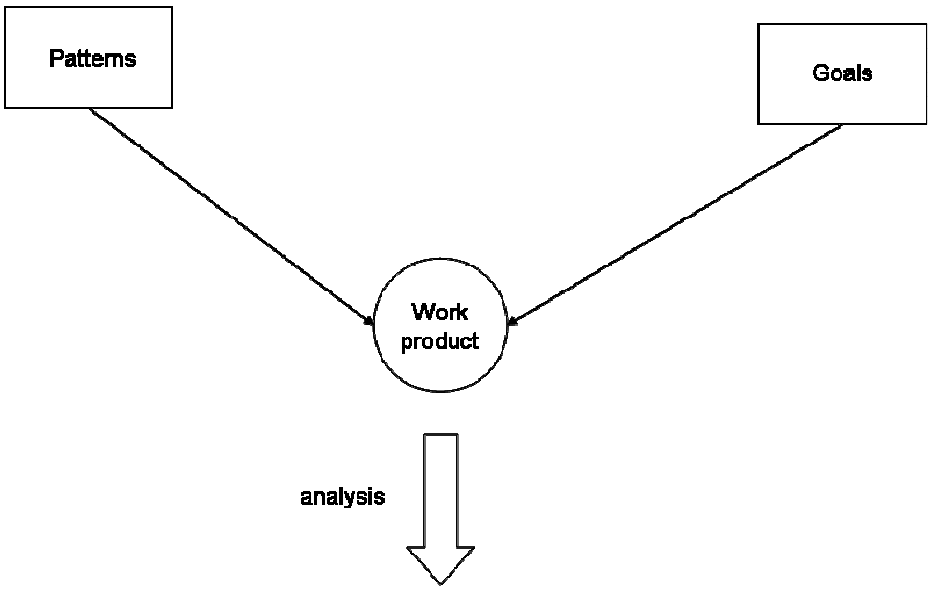

Figure 28: Goal-driven and pattern-driven analysis

8.4 Determining interoperability domain

In discussing an organisation or system's ability to interoperate, it is important to consider the environment in which it operates and the respective environments of other organisations/systems with which this organisation/system interacts. This is because different environments imply different considerations that apply to the organisations/systems therein.

Examples of such considerations are:

- various types of governance rules, arising, for example, from privacy laws, national or international regulations, or legal or organisational

policies; these rules typically reflect social, economic or sometimes cultural conditions from the environment;

- limitations associated with the skills and capabilities of people involved, e.g. clinical knowledge or technical standards awareness;
- professional norms of an environment, such as an agreed use of certain clinical terminology with its own semantics and syntax;
- technology requirements, such as 24x7 connectivity, bandwidth and reliability, as well as physical and temporal constraints that vary from environment to environment.

These different considerations imply different interoperability goals.

NEHTA uses the term *interoperability domain* to refer to the boundaries enclosing a set of co-located constraints. NEHTA distinguishes between local, enterprise and community (more precisely, a healthcare community) domains, as elaborated below and depicted in Figure 29.

Note that, as far as the interoperability domain is concerned, a specific organisation/system should be characterised by each of these boundary types simultaneously, e.g. a state health organisation is an enterprise in its own right (enterprise domain), with many constituent units (local domains), but is also part of a national health community (e-health community domain).

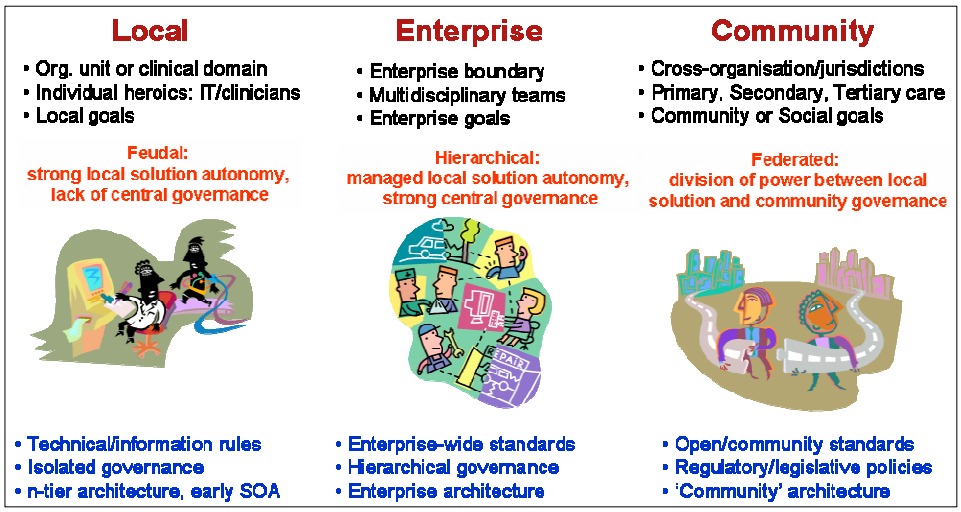

Figure 29: Interoperability Domain

The sections below describe in more detail the characteristics of these different domains of interoperability and typical approaches adopted to address interoperability challenges in each of these.

8.4.1 Local

A local domain exists within one or more enterprise or community domains and can denote a specific boundary type, e.g. geographical, organisational, clinical, and IT application domain boundary.

Some examples are:

- an organisational unit in a large healthcare organisation;
- a GP practice as part of a medical centre;
- an individual GP in a remote community (which in turn is part of a state/territory jurisdiction);
- a voluntary non-government organisation in a natural disaster area;
- day surgery unit as a part of a broader surgical department or a cardiology unit as part of a broader internal medicine department.

Note that the relationship between the three domains is not strictly hierarchical and the interoperability goals of a local domain reflect local concerns and impacts with little regard for broader issues. On the other hand, interoperability issues within a broader boundary (e.g. enterprise or community) are likely to influence local interoperability requirements.

8.4.1.1 Goals

There are a number of characterising features and solution approaches to interoperability within the local domain.

First, an individual, an organisation or a system in a local boundary is typically focused on achieving *local goals*. There are varying (typically not high) levels of awareness or concerns as to how these goals might be aligned with the goals of a broader domain, as the following two examples illustrate:

- an IT manager in a hospital's audiology department is choosing and configuring a commercial hearing test product with new audio testing capability. There may be little concern for the needs and requirements of larger clinical information systems within the hospital environment. The local interoperability issue is often regarded as a closed world of applications needing to work together in a local context. It should be noted that the "closed world" view is unrealistic as most systems will exist simultaneously within a broader enterprise and community domain.
- a software integration team in a hospital may begin to use SOA principles to support existing system integration practices (e.g. the use of interfaces to separate functional definitions from implementation); although their focus is on integration between existing legacy systems, they will need to have an increasing awareness for needs of architectural alignment with other systems in the hospital.

These two examples demonstrate different dependency strengths between local and enterprise boundaries, both of which however exemplify *strong local solution autonomy*, although in the second example, taking into account enterprise-wide goals.

Second, the interoperability within a local domain may initially be championed by certain individuals, whether IT experts or clinicians, who initiate efforts in starting or improving interoperability with others. This *individual heroics*, if proven to deliver local goals, and when motivated by broader social or economic goals[26], can be an important impetus towards repeating interoperability solutions in a broader, enterprise or community context, thus achieving enterprise or community goals. It is worth noting that such a change in perspective may be driven in this manner from bottom-up, or otherwise as a management imperative, top-down. This choice of approach (even a combination of approaches) is driven by the buy-in of the stakeholders themselves into the interoperability agenda.

Third, the local domain can be characterised by *isolated* or *limited central governance*. This can be due to an inherit nature of the boundary, as in established strong local governance of a GP practice within a medical centre, or due to organisational issues such as an increasing, though often undesirable, strengthening of local control.

In many respects, the local domain, being characterised as strong local solution autonomy with isolated central governance, can be likened to a feudal system of government (see Figure 29).

[26] Note that there is anecdotal evidence of pursing local goals at the expense of enterprise or community goals, and the appropriate governance policies need to be established to address this problem.

8.4.1.2 Approaches to interoperability

In addressing interoperability challenges within the local domain there are a number of possible approaches such as:

- Adoption of a locally agreed set of principles, rules and standards, to facilitate technical and information *integration* and broader set of local *interoperability* requirements e.g. an adoption of sound architectural approaches, such as n-tier architecture or SOA;
- An agreement on the best local common processes, standards and other local approaches developed to enable multiple systems to interact at a local level.

Note that where required (and possible) each of these approaches may need to take into account external requirements, either from the enterprise or community domain in defining the respective rules and standards. For example, if enterprise interoperability is adopted then it will impact on the set of existing local interoperability approaches. Further, these solutions can address interoperability challenges in the short term, but may not be sufficient in the long term, when enterprise or community approaches need to be applied.

8.4.2 Enterprise

An enterprise domain denotes a boundary of a single organisation, recognised as a legal entity, irrespective of its size, organisational or geographical structure. Examples are:

- Government-funded healthcare organisations, such as public hospitals, community centres, outpatient clinics, as well as state or territory jurisdictions as a whole; note that some larger organisations can consist of many units or departments, which define their own enterprise domain
- Private health organisations, such as private hospitals, pharmacies, pathology providers, dental services, or GP practices;
- Other non-government organisations.

8.4.2.1 Goals

Each of these organisations is created to achieve certain *enterprise goals*, which in turn influence the organisation's policies, processes and structure. In the health sector, enterprise goals may be mainly motivated by social objectives as in public hospitals, or they may be motivated by a combination of commercial and social objectives, as in private hospitals.

As opposed to local boundaries, where the interoperability is typically driven by individual efforts (or small teams), with a focus on a limited problem domain, the enterprise domain requires a more coordinated approach. This is because it is driven by a collective effort, involving *team work* while being focused on a problem of enterprise-wide significance. For example, if a hospital is the enterprise in question, an example would be multidisciplinary teams that contribute to the holistic care of patients within a particular speciality, e.g. immunology. Note that the enterprise boundary can be of a broader domain, such as a whole state health department or as narrow as a hospital or a general practice.

Governance structures in enterprises are typically *hierarchical*, with different strengths and depths of hierarchy, while keeping *guided local solution autonomy* when dealing with local interoperability problems (see Figure 29). Thus a key characteristic here is the singularity of the point of control and in this respect the enterprise domain can be likened to an autocratic (i.e. hierarchical) system of government.

Note however that some organisations operate as a collective, with federation structures linking these points of control. Examples include

- a State health service that comprises several area health services which are all autonomous, but report to a State health department,
- the Australian Federation of AIDS organisations,
- the Australian Federation of Disability Organisations, within national boundaries, or
- the World Health Organization or the International Committee of the Red Cross at an international level.

8.4.2.2 Approaches to interoperability

In order to address enterprise interoperability challenges, several approaches can be taken, such as:

- Adoption of an agreed set of enterprise-wide standards, whether based on recommended principles and solutions from official standards, or defined by the organisation to satisfy its own requirements.
- Establishment of an enterprise architecture program to address various architectural concerns, covering business architecture, information architecture, application architecture, and technical architecture, as well as to establish enterprise architecture processes and governance.

Note that such mechanisms are described as part of the *Supporting National E-Health Standards Implementation: Adoption, Uptake & Implementation* [Standards-I] document.

8.4.3 Community

A community domain denotes a boundary within which a number of enterprises or individuals interact, in order to fulfil some *shared goal*, while at the same time meeting their individual needs or local/enterprise goals.

In healthcare, a *healthcare community* is typically centred on the delivery of safe and reliable healthcare to individuals, while an *e-health community* is a healthcare community empowered by the use of ICT to improve safety and reliability, and add convenience to healthcare delivery.

Note that the community domain has a far more open boundary condition as opposed to enterprise and local domains that tend to be more inwardly focussed. This implies that membership and relationships within the community are relatively unencumbered as the community responds to the needs for collaborative healthcare delivery and alternatives.

A shared goal is defined by some authority, typically a government[27], with the aim of satisfying some social goal, or by the members who are establishing the community, to provide mutual benefits, as in many mutual agreements and business contracts.

As in the case of the enterprise domain, a community goal will define policies, such as privacy policies, that govern interactions in a community, to ensure predictability, fairness and trust.

8.4.3.1 Goals

While interoperability within an enterprise domain is 'inward' focused, interoperability in a community is concerned with the interactions between enterprises and interactions which cross jurisdictional boundaries.

[27] A good example for setting such a social goal is the decision of the Australian Government in 2004 to progress an interoperable e-health environment in Australia to satisfy the broader healthcare goals for Australian population. Interoperable e-health can be regarded as a shared goal for the Australian health community and NEHTA has been tasked to facilitate the accomplishment of this shared goal.

For example in supporting chronic disease management for a patient, information may need to be exchanged

- among many healthcare organisations and systems;
- within primary, secondary and tertiary sectors;
- involving both the public and private sectors; and
- involving international entities, in certain extreme cases.

Such an exchange of information needs to respect policies and guidelines set by a chronic management community, e.g. privacy policies, continuity of care guidelines for chronically ill patients, or even policies governing interactions with non-government organisations.

Within the community domain, community members change more often and have more differentiation than those within an enterprise.

Within the community domain, governance is typically established by following the principle of *federation*, which recognises the existence of *independent domains* governed by their own authorities, while providing agreed interaction standards between these domains (see Figure 29). These agreed approaches are either specified through a set of policies established by national or international authorities or by agreements between authorised representatives from these domains. Note that each domain's authority provides governance for that domain. For example, a domain's authority can define funding policies covering conditions under which healthcare services in this domain are to be delivered by the providers in the domain, including required accreditation and reporting policies. Both the domain authorities and federation agreements contribute to community governance.

A community domain can thus be characterised by division of power between 'local solutions' and community governance, where 'local solutions' (to interoperability problems) could be either related to the enterprise or local domain.

8.4.3.2 Approaches to interoperability

In order to address challenges associated with interoperability within a community domain, several possible approaches could be adopted, including:

- the adoption of open standards published by Standard Development Organisations or community standards that are agreed by individual communities, augmented by clearly defined certification processes and governance at the community level (national or international);
- the establishment of a clear policy framework covering regulatory and legislative policies or business contract policies that ensure satisfaction of community goals, and ensure compliance of each member of the community with such policies;
- the establishment of a 'community architecture' program, consisting of an agreed set of concepts and principles which, when respected, will provide a consistent architectural approach at the community level, as a necessary condition for community interoperability.

8.4.4 Summary

This section has introduced a distinction between the local, enterprise and community domains, because these boundaries define different characteristics of relevance for interoperability. However, these boundaries are often not so sharp and thus the separation of local, enterprise, and community domains forms a continuum. For example, one should apply community interoperability approaches (listed in section 8.4.3.2) in an enterprise because the organisation operates as a collective rather than a strict hierarchy of control. The distinction between enterprise and community then becomes one of underlying environmental factors rather than simply applying an

organisational moniker. In fact, some communities in name may in fact operate much like a typical enterprise due to their singularity of control structure.

It is also important to state that:

- An organisation will need to address all three different contexts at the same time, thus having a 'localised', 'inwards' and 'outwards' views on interoperability.
- Each of the local, enterprise and community domains can be represented by the IF community concept, with distinct goals, governing policies, including conformance and compliance requirements and adopted processes and interactions.
- While local and enterprise interoperability have been addressed in the context of various technical approaches, including integration solutions and architectural approaches, community interoperability is becoming an increasingly important challenge, in particular in the domain of e-health.
- The cost of community governance is often higher than that of enterprise governance as more effort is required to facilitate a federated approach rather than a more efficient centralised point of control.

9 Interoperability Maturity Model

The previous sections have pointed at many interoperability challenges and several approaches to tackle the interoperability problems. They highlighted the role of ICT systems as an important enabler in empowering healthcare providers, individuals and organisations in their ability to interoperate to deliver patient-centric services. This is in spite of different organisational and jurisdictional boundaries. This ability will significantly influence organisational capability to deliver safe, reliable, efficient and convenient healthcare services. The term *e-health interoperability* is used to signify an overall capability of all participants to interoperate, spanning information, technical, and organisational perspectives [IF].

This mix of interoperability perspectives is inherently complex and the complexity is further exacerbated by a need for a *continuous state of readiness* for adoption of new technologies, as well as the need for better information quality and the introduction of new clinical/administrative processes and policies. Capability maturity models are applied in other industries to drive quality practices in complex fields of endeavour. This is equally desirable in the health IT community. In fact, it is recognised that there is a pressing need for an *e-health interoperability maturity model,* a comprehensive model for defining a managed path towards increasing e-health interoperability, including the assessment of that ability [Rubin].

This section outlines key points from the e-health interoperability maturity model proposed by NEHTA [IMM]. This model is aimed at helping e-health organisations[28] improve their ability to use or deliver interoperable e-health systems[29], with the ultimate goal of increased healthcare benefits - in particular improving safety, quality and effectiveness in the delivery of healthcare services.

9.1 Key components

The IMM closely follows the Capability Maturity Model Integration (CMMI) reference model and consists of the following IMM components:

- *interoperability maturity levels*. There are 5 levels, namely: Initial, Managed, Defined, Measured and Optimised. Reaching each level requires the attainment of the previous levels;
- a set of *interoperability goals,* identified within the e-health domain. These goals are separated into interoperability perspectives, as introduced in section 8.1
- an *assessment framework,* to measure the maturity level of an e-health organisation or to assess the interoperability of an e-health system[30].

The application of CMMI is a process of continual improvement that links goals, practices, and work products as described in Figure 30. Goals influence organisational practices that in turn are demonstrated in the work products that are produced or procured. A *work product interoperability assessment* ensures the products do indeed reflect desired goals and *interoperability maturity assessment* checks that organisational practices are delivering

28 Examples of e-health organizations are ICT departments within jurisdictions, vendors involved in delivering e-health systems and services, and various standards development organisations or other associations concerned with the design, development and use of e-health systems.

29 Informally, an e-health system is a solution within the health sector which, to different levels, rely upon ICT capabilities.

30 Note that, although the assessment of e-health systems interoperability is likely to reflect the maturity of processes established to deliver interoperability, this assessment can be done independently, for purposes other than defining process improvements.

interoperable outcomes. The IMM is based on the same improvement approach as CMMI and the dependencies between these sequential steps should be kept in mind throughout the rest of this section.

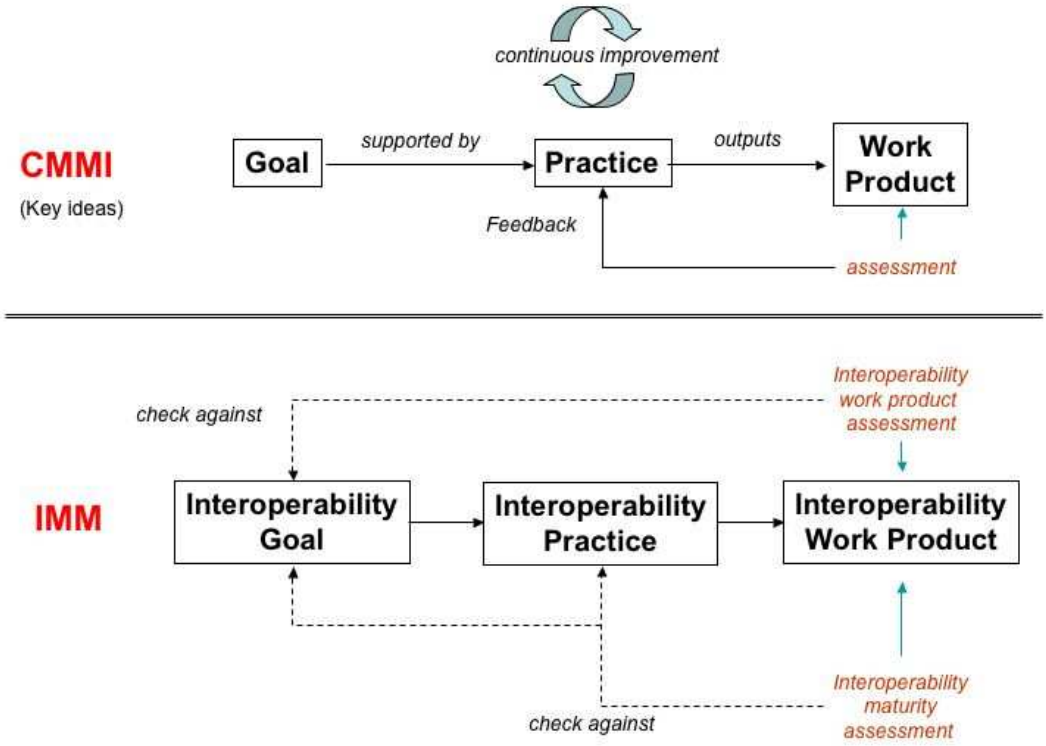

Figure 30: The CMMI and IMM continuous improvement processes

9.2 Interoperability Maturity Levels

CMMI was chosen as a reference framework because of its general applicability to any problem domain (or target) for which maturity models are to be developed[31].

Accordingly, five levels of maturity are defined to capture the maturity of practice (see also Figure 31):

- *Initial*: There is an early awareness of e-health interoperability requirements and characteristics and perhaps some early e-health interoperability solutions adopted, typically localised within certain clinical or administrative domains (as these provide environments with limited complexity).
- *Managed* (or under development): An organisation will begin accomplishing some interoperability goals, such as the adoption of specific e-health standards, while gaining an early shared understanding of data, services or internal processes, as well as initial governance established to ensure repetition of earlier successes.
- *Defined*: An organisation has defined a set of guidelines for the adoption of e-health standards for data, services and processes, according to the lessons learned from previous maturity levels. These are further augmented with explicit focus on policy and legal compliance. Governance is well defined and defined levels of organisational readiness for interoperability outcomes are established. Communication standards for interaction with internal and external partners are

[31] Although CMMI is used in this document to focus on the interoperability goals of an e-health system, it can be also applied in a broader e-health context, covering other e-health system characteristics such as feature set, quality and change management.

established as are the supporting organisational structures facilitating a shared understanding across technical and semantic issues.

- *Measured*: An organisation has established processes for appraising and measuring e-health interoperability. This can be done before the system is deployed such as through conformance and compliance activities or during the operation of the system, i.e. run-time monitoring.
- *Optimised*: The organisation has implemented processes to support continuous interoperability improvements, driven by feedback from monitored processes, with the aim of improving overall e-health interoperability capability.

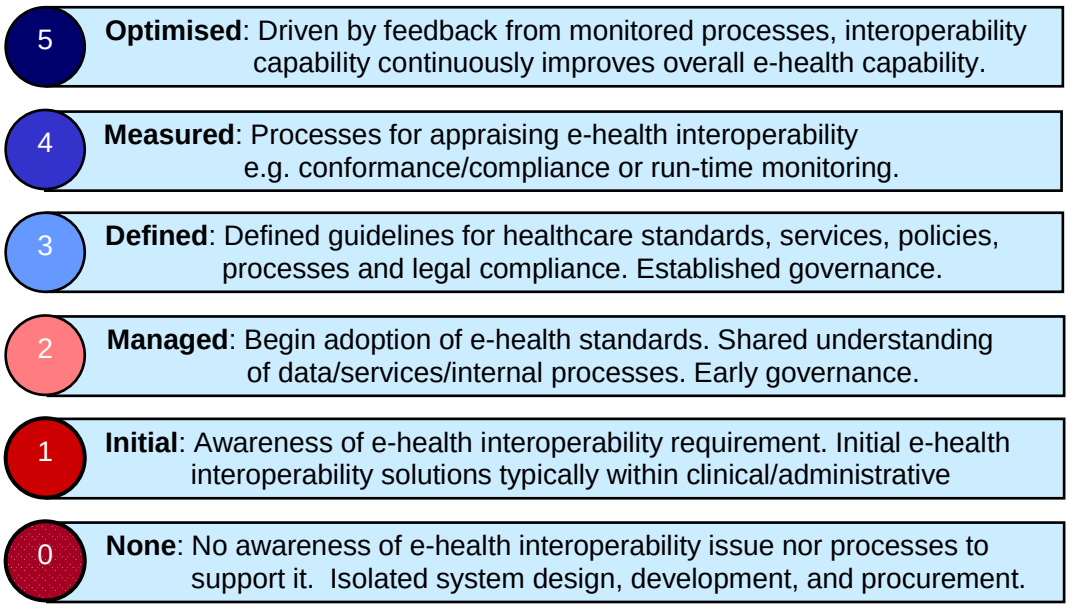

Figure 31: Interoperability maturity levels

The consistent use of this approach supports a *shared understanding* of maturity between organisations. Each of the levels in Figure 31 defines an increasing level of maturity that can be used to define specific interoperability maturity goals that in turn can be analysed in terms of practices that need to be established to provide continuous improvement in interoperability (see Figure 30). In order to measure the success of interoperability outcomes, one must have already defined the standards for that success.

It is important to note that above level 1 (Initial) each maturity level requires the accomplishment of goals defined in previous levels.

These maturity levels have general applicability and can be further refined to reflect the specific context for analysing interoperability, namely the local, enterprise or community interoperability domains. Figure 32 describes examples of different interoperability practices within the three different domains. For instance, it shows how service oriented architectures (SOA), enterprise architectures (EA) and community architectures are used within different domains to address the respective interoperability challenges. This may range from efforts of early champions to adopt some technical or information interoperability within an enterprise boundary to an established certification program and monitoring of Service Level Agreements (SLAs) governing rules within the e-health community.

Note that some cells within the local domain are left empty as it is not clear that higher levels of maturity have a cost-benefit value at this granularity.

	Local	Enterprise	e-Health Community
5		Continuous interoperability improvement Enable organisational goals Inward and outward: EA as a binding process	Continuous interoperability innovations Enables Community/Social goals Emergence, dynamics, adaptation
4		Impact of EA/SOA on organisational goals Identify interoperability weak points	Established Certification program Community SLA monitoring
3	Local standards governance Early architecture principles	Enterprise-wide standards/governance Generic EA principles augmented with SOA Early organisational interoperability	'Community' architecture Interoperability governance defined Governed use of open standards
2	Shared early interoperability experience ICT standards adopted	Some defined EA processes Business and IT committed to EA	Interoperability frameworks Community/National collaboration Governance in development
1	Technical integration efforts Ad-hoc solution architecture	Individual champions for technical and information interoperability Efforts underway for executive EA buy-in	Community interoperability vision Policy makers delivering social benefits Ad-hoc use of standards
0	Isolated design/development Siloed procurement	No interoperability awareness No processes to support EA	No processes to support cross-organisational interoperability

Figure 32: Interoperability maturity: different domains

9.3 Assessment Framework

This section provides a sequence of steps for applying the IMM to address organisational requirements for improving interoperability.

These steps constitute a recommended interoperability assessment methodology for applying the IMM to the problem of national e-health interoperability, as depicted in Figure 33. Note that this methodology can also be applied in the context of enterprise interoperability.

The first step is to clearly identify the *interoperability target* of interest. Usually, this is an e-health organisation for which an interoperability maturity model is to be developed, but this can also be an e-health system for which interoperability assessment is to be carried out. These two interoperability targets are typically intertwined as part of a comprehensive interoperability maturity program, but they are described here as two applications of the IMM.

This is to be followed by identification of the *interoperability domain* for the target, i.e. local, enterprise or community domain. The domain highlights the boundary condition for issues of relevance and ensures issues of a broader context are appropriately balanced against local needs.

These two steps are followed by identifying relevant *interoperability goals* for the target within the domain, using the national interoperability goals identified in section 8.1 as a starting point. Note that not all goals have the same importance and individual importance weightings should be assigned (e.g. high, medium, low) to each goal. These weightings can be used to focus the assessment on important goals first, or to select priority organisational practices for interoperability maturity program planning. In the second case, the selection process could also be driven by the results of a lightweight cost-benefit analysis, undertaken for the purpose of assessing costs and benefits of interoperability, or for broader e-health benefits realisation purposes. This is beyond the scope of this document.

In the case of a maturity assessment for an e-health organisation, the IMM also requires that the *interoperability practices* used to accomplish the interoperability goals be defined and assessed. That is, each interoperability

practice should be explicitly linked to a set of interoperability goals, and the interoperability assessment should identify the success or failure of these practices in attaining the interoperability goals, typically by assessing outputs of those practices.

Maturity assessments of either organisations or e-health systems will typically identify the need for an interoperability maturity program (see right hand side of diagram in Figure 33).

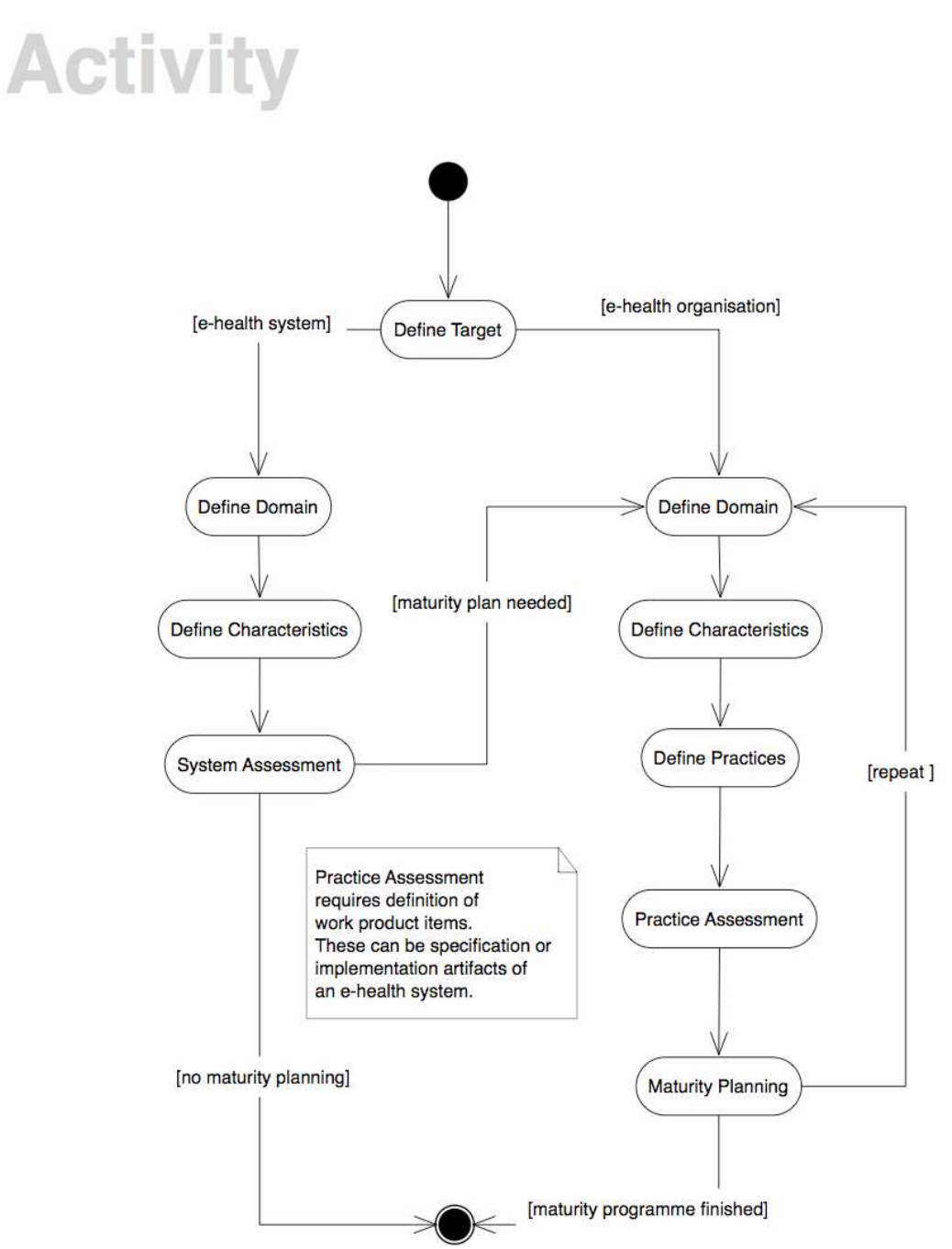

Figure 33: Assessment framework

9.4 Interoperability Maturity Planning

The assessment of organisational practices will define a set of processes that support the creation of interoperable outcomes by an organisation. These practices can be summarised according to organisation, information, and technical areas (note that common processes should be allocated to their corresponding perspective). The maturity planning worksheet, below, will

include this static organisational evaluation and will then define additional practices required to take each of the organisation, information, and technical interoperability areas into the future with higher levels of interoperability practices, effectively defining the organisation's interoperability maturity program. It can be useful to present the maturity planning worksheet as a series of three tables, each allocated to one of the interoperability perspectives.

Maturity Level	*Organisation*	*Information*	*Technical*
5			
4			
3			
2			
1			

Table 3: Maturity planning worksheet

9.5 Summary

This section has outlined key ideas from the first version of the interoperability maturity model (IMM) developed by NEHTA and presented in [IMM].

The IMM was developed taking into account recommendations from the CMMI model and was tailored for the needs of the e-health environment. The e-health domain is reflected in the definition of the maturity levels chosen. They refer to an increasing ability of organisations to support interoperability in e-health. These different maturity levels are of a generic nature and can be further tailored for the specific interoperability domain in question, whether local, organisational or community.

The IMM also introduced a methodology that can be used to assess interoperability of e-health systems or organisational practices in support of interoperability processes.

This version of the IMM might require further refinement to better reflect the CMMI recommendation or needs of the e-health environment.

10 Standards Catalogue

The National E-Health Standards Catalogue (Standards Catalogue) consists of a collection of standards and specifications that are essential guidance for those who develop, sell, support, buy and implement e-health software in Australia. The catalogue provides a list of the standards recommended by, and specifications sourced, developed and recommended by, NEHTA. The catalogue also provides advice on when and where the use of a standard is appropriate.

The Standards Catalogue is displayed online or can be downloaded from the NEHTA website. It is updated regularly as NEHTA's work progresses. Updates are reflected in the version number of the catalogue.

10.1 Importance of Standards

Standards are relevant to all areas of NEHTA's work, and provide rigour as well as a means of validation with external expert groups.

The lack of clear standards makes it difficult for vendors to develop software applications that can support a broad range of communication within the health community. Vendors face developing their own solutions and accepting the risk of industry adopting a different approach. Where widely supported standards are available to vendors, the lack of agreement at a national level about their use can preclude their adoption.

Standards also benefit those who purchase and implement health software applications. Knowing which software products conform to agreed standards can greatly simplify the purchasing process, and increase purchaser confidence that the selected product will be fit-for-purpose. Standards also offer the potential to avoid vendor “lock-in”.

10.2 Selection Criteria

Standards and specifications within the catalogue are those that are either currently in use or recommended for use by NEHTA. The catalogue will provide links to both de facto and de jure standards from national and international standards bodies including proprietary, business, and more openly developed standards.

NEHTA supports the adoption of open standards where appropriate. These standards should require no royalty payments, be openly published, allow extension, promote reusability, and reduce the risk of technical lock-in and high switching costs. Open standards will therefore be selected by NEHTA where possible. However, where open standards are not appropriate due to significant market or technical issues, NEHTA will adopt the standards deemed most fit-for-purpose, relevant and useful to the community.

NEHTA’s analysis and development process is rigorous and aligns with the Code of Good Practice for the Preparation, Adoption and Application of Standards that is annexed to the World Trade Organization (WTO) Agreement on Technical Barriers to Trade. NEHTA undertakes significant analysis for the standards it recommends and specifications it develops by ensuring that the end product is fit-for-purpose and aligns with NEHTA’s recommended architectural approach.

The process for development of specifications and recommendation of standards involves significant consultation with jurisdictions and industry to ensure that the work receives feedback and advice from suppliers, developers, purchasers and implementers i.e., end users of the work.

NEHTA's development process for the building blocks also ensures that appropriate standards are used at every stage of the process – ensuring that all of NEHTA's work outputs align with the Code of Good Practice. [32]

10.3 Conceptual Model

The Standards Catalogue Menu provides links to the following menu structures which are available for viewing the catalogue:

- Domain;
- Interoperability Framework; or
- Archived.

The whole catalogue is available from the Domain or Interoperability Framework view. It is a method to breakdown the catalogue to suit different audiences, or approach the same information from different perspectives.

10.3.1 Domain

The Domain path classifies the standards and specifications corresponding to NEHTA's program of work, for easy access. The following are available:

- E-Health Interoperability;
- Clinical Communications including the following aspects of NEHTA's work:
  - Clinical Terminologies;
  - Clinical Information Specifications;
- Unique Healthcare Identification including NEHTA's work on the:
  - Healthcare Provider Identifier;
  - Individual Healthcare Identifier;
- Identity Management;
- Secure Messaging;
- Shared Electronic Health Record;
- Supply Chain; and
- Engagement and Adoption.

Each section displays only the relevant recommended standards and specifications for the selected domain. Standards and specifications which are used by more than one domain are repeated under each relevant domain.

10.3.2 Interoperability Framework

The Interoperability Framework path divides the standards and specifications and then classifies them within the perspectives of the Interoperability Framework. The following paths are available:

- Organisational;
- Informational; and
- Technical.

Similar to the domain path, each perspective displays only the relevant standards and specifications, repeating where necessary.

[32] NEHTA, 2007, *Supporting National E-Health Standards Implementation – Adoption, Uptake and Implementation v-1.0,* National E-Health Transition Authority Ltd, Sydney, p. 18.

10.3.3 Archived

The Archived path displays all standards that were once part of the catalogue but have been deprecated or superseded.

10.4 Standards Information

Each standard includes the following metadata information:

- *Identification number* and title of the standard/specification;
- *Date of publication*;
- *Status* of the standard within the standards community e.g., Draft, Current, etc.;
- *Custodian* of the standard/specification e.g., ISO, NEHTA;
- The *Committee/Initiative* responsible for the development of or ongoing work on the standard/specification;
- *Type of resource*, i.e. NEHTA developed specification, or Standard;
- *Link* to the standard/specification on the custodian's website;
- *Overview* - A short overview of the standard/specification;
- *Motivation* - Reason the standard was included in the Standards Catalogue;
- *Usage criteria* - The NEHTA recommended criteria for where/how the standard is applied; and
- *Comments* - Other relevant comments.

Where the standard/specification applies to more than one domain, the motivation and usage criteria will reflect this difference.

Further information in the form of links is also available including:

- *Initiatives links:* links to Overview and Downloads of the NEHTA initiative/s relevant to the domain;
- *Supercedes:* links to another standard/specification that the viewed standard/specification has superceded which is also in the catalogue;
- *Superceded by:* links to another standard/specification that the viewed standard/specification has been superceded by which is also in this catalogue;
- *Equivalent:* links to an equivalent standard or specification e.g. an Australian Standard that is equivalent to an ISO Standard, which is also in the catalogue;
- *Series:* links to other standards or specifications within the same series.
- *Other:* Any other related standard or specification that should be considered when looking at the current standard/specification.

11 Next Steps

The Interoperability Framework is a living document that is continually updated as a result of new development ideas and in response to the experience gained in implementing e-health systems.

At present, several areas need to be addressed:

- Provide a formal expression of interoperability languages, most likely in the form of language meta-models and based on the UML formalism; this is of relevance for the use of tools to support interoperability modelling;
- Provide a structured catalogue of interoperability patterns and update a number of existing pattern categories, in particular those related to legislative policies, governance and value assessment categories;
- Establish mapping between specific modelling concepts of the IF and the modelling concepts from relevant clinical or messaging standards and specifications such as HL7 Reference Information Model [HL7], Clinical Document Architecture (CDA) [CDA] and CEN/TC251 Health Informatics Service Architecture [HISA];
- Identify and extract those fundamental modelling artefacts which are present in more than one of the interoperability perspectives, such as quality, behaviour, identity, service and policy; this is needed to provide better alignment between concepts and patterns from different perspectives and is of significance for the use of software tools to support design and management of interoperability artefacts; note that this version of the IF began this process by separating certain fundamental interoperability principles (in section 2.2.1) and goals (referred to as 'common' goals in section 8.1.1);
- Analyse and adopt a set of tools in support of interoperability modelling; these tools would need to support the full life cycle of the interoperability methodology, covering requirements, specification, certification and value assessment stages; ideally the tools will be of a similar scope to the tools to be used to support work of business analysts, enterprise and solution architects, as well as developers and testers;
- Update and consolidate the interoperability maturity model to reflect best international practices in the area, and in response to the experienced obtained from its application within the Australian e-health context.

In addition, the next version of the IF will need to continue:

- Collecting and documenting interoperability patterns based on case studied undertaken in the context of concrete e-health projects; these need to be stored in a patterns repository, in a similar way as architectural patterns are stored in enterprise architecture repository (captured as enterprise continuum in the TOGAF standard);
- Capturing the suggestions of e-health experts about a new or updated sets of interoperability goals;
- Gathering feedback from enterprise and solutions architects about the validity of existing interoperability concepts, and where needed, refine or extend these concepts;
- Identifying additional guidelines and techniques to support the implementation of interoperability solutions of relevance for the conformance, compliance and accreditation program, interoperability maturity modelling and enterprise architecture.

12 References

[AGTIF] Australian Government technical Interoperability Framework, July2005, available at: http://www.agimo.gov.au/publications/2005/04/agtifv2

[Alexander] Christopher Alexander et al., A pattern language: towns, buildings, construction, Oxford University Press, 1977

[ANAO] Better Practice Guide to Public Sector Governance, http://www.anao.gov.au/

[BCG] National Health IM&ICT Entity – Business Case, Draft V3.0, 7 December 2004.

[BRP] J. Thorp, The Information Paradox, Realizing the business benefits of information technology, McGraw Hill, 1998.

[CDA] R.H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F.M. Behlen, P.V. Biron, A. Shabo, HL7 Clinical Document Architecture, release 2, Journal of the American Medical Informatics Association, Vol 13, Number 1, Jan/Feb 2006.

[CMM] The Capability Maturity Model for Software http://www.sei.cmu.edu/cmm/

[CMMI] Capability Maturity Model Integration http://www.sei.cmu.edu/cmmi/

[Discharge] National Discharge Summary, Data Content Specifications, Version 1.0 – 21/12/2006, NEHTA.

[DOC] http://www.osec.doc.gov/cio/arch_cmm.htm

[eGIF] Setting Standards for Seamless Electronic Government, http://www.govtalk.gov.uk, June 2005.

[EDOC98] P. Linington, Z. Milosevic and K. Raymond, "Policies in Communities: Extending the ODP Enterprise Viewpoint". Proc. 2 nd IEEE Enterprise Distributed Object Computing Conference, EDOC98.

[EDOC02] Z. Milosevic, A. Jøsang, T. Dimitrakos and M.A.Patton. Discretionary Enforcement of Electronic Contracts. Proc. of the 6th IEEE International Enterprise Distributed Object Computing Conference (EDOC 2002).

[EIF] European Interoperability Framework for Pan-European eGovernment Services, Version 1.0, EC 2004

[EPAN] Key Principles of an Interoperability Architecture, European Public Administration Network eGovernment Working Group, 2004.

[Fowler] www.martinfowler.com/eaaDev/TemporalProperty.html

[GOF] E. Gamma, R. Helm, R. Johnson, J. Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software (Addison-Wesley Professional Computing Series), 1994.

[HIPF] Health Informatics Profiling Framework, 2001-12-7, ISO TC 215

[HISA] Health Informatics — Service architecture — Part 1: Enterprise viewpoint, CEN/TC 251, prEN 12967-1, Date: 2005-05-09

[HL7] http://www.hl7.org./ (last visited 2007-8-10)

[HL7 Interop] Coming to Terms: Scoping Interoperability for Health Care, HL7 EHR Interoperability Work Group, 16 January, 2007.

[HP] Andrew Pugsley. "Assessing Your SOA Program." HP.com. Accessed online 27 Oct 2006. (ftp://ftp.hp.com/pub/services/soa/info/4AA0-4824ENW.pdf.)

[IBM] Arsanjani, A., Kerrie Holley. "Increase Flexibility with the Service Integration Maturity Model (SIMM)." www-128.IBM.com.

[IBM patterns] http://www.ibm.com/developerworks/patterns/index.html

[IdMResSet] Identity Management Resource Set, version 1.0, National E-Health Transition Authority, August 2007.

[IEEE Dist Sys] IEEE Distributed Systems Online (http://dsonline.computer.org/portal/ (last visited 2006-02-15.)

[IEEE] Medical Records: From Clipboard To Point-and-Click, The Institute, IEEE, December 2005.

[IF1.0] NEHTA Interoperability Framework, 1.0 available at http://www.nehta.gov.au/.

[IMM] Interoperability Maturity Model, version 1.0, National E-Health Transition Authority, March 2007.

[InfoWay] http://www.infoway-inforoute.ca/en/home/home.aspx (last visited 2007-06-13.)

[InfluenceDiag] www.lumina.com/software/influencediagrams.html (last visited 2005-11-02.)

[Linington] P.F.Linington and W. Frank, Specification and implementation in ODP, proc. 1st workshop on Open Distributed processing, Portugal, July 2001.

[IOM] http://www.iom.edu/) (last visited 2006-02-13.)

[IT Gov] Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, http://www.itgi.org/ (last visited on 2007-06-20)

[LISI] Kasunic M, Anderson W., Measuring Systems Interoperability: Challenges and Opportunities, Technical Note CMU/SEI-2004-TN-003

[MDA] Model Driven Architecture, http://www.omg.org/mda/

[NEHTAIF1.8] Towards an Interoperability Framework v1.8, National E-Health Transition Authority, August 2005.

[NEHTA BR] Paths to Benefits, version 1.0, National E-Health Transition Authority, August 2006.

[ODP-EL] ISO\IEC IS 15414, Open Distributed Processing-Enterprise Language, 2002

[ODP-RM] ISO/IEC 10746-1 10756-2 10746-3 10746-4 Basic Reference Model for Open Distributed Processing.

[OMG] Object management Group, http://www.omg.org, June 2005.

[Ont] http://www.ices.on.ca/file/Scorecard_report_final.pdf

[PC-Aug05] Impacts of Advances in Medical Technology in Australia, Productivity Commission's report, 31 August 2005.

[Porter] Redefining Health Care: Creating Value-Based Competition on Results , by M. E. Porter, E. O. Teisberg, Harvard Business School Press, 2006.

[Priv] Privacy Act 1988, Act No. 119 of 1988 as amended on Dec30, 2006.

[Rector] A. Rector, Clinical Terminology: Why is it so hard?, 1999 Methods of Information in Medicine 38(4):239-252

[RefLandscape] The Referral Landscape, An Overview of referrals in Australia, V1.0, 2007-01-27, NEHTA internal document.

[Rubin] Rubin K, Why Measure Interoperability? http://krubin.blogspot.com/2006/06/why-measure-interoperability.html

[Schrenker] Software Engineering for Future Healthcare and Clinical Systems, IEEE Computer, April 2006, p.27-32.

[SixSigmaH] healthcare.isixsigma.com/library/content/c030513a.asp

[SNOMED] http://www.snomed.org/ (last visited 2005-11-10)

[SOA] OASIS SOA Reference Model TC, last visited on 2005-Sep-28

[Spirivulis et al] Australia needs a national health information nomenclature, discussion paper, 2005.

[Standards-I] Supporting National E-Health Standards, version 1.0, Implementation, National E-Health Transition Authority, February 2007.

[Standards-M] National E-Health Standards Development: A management framework, version 1, National E-Health Transition Authority, March 2006.

[TOGAF8.1] http://www.opengroup.org/togaf/

[UML] Unified Modelling Language, http://www.uml.org/

[UML ODP] Information technology — Open distributed processing — Use of UML for ODP system specifications, ITU T Recommendation X.906 | ISO/IEC 19793 (Final Draft International Standard)

[Walker] Walker et al., "The Value of Health Care Information Exchange and Interoperability", Health Affairs: The Journal of the Health Sphere, 19 January 2005.

[WS-Policy] http://www.w3.org/TR/ws-policy/

13 Glossary

CDA	Clinical Document Architecture
CIS	Clinical Information System
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EDA	Event-Driven Architecture
ICT	Information and Communications technology
IF	Interoperability Framework
IIF	Information Interoperability Framework
ISO	International Standards Organisation
IT	Information Technology
GP	General Practitioner
MOM	Message-Oriented Middleware
NEA	NEHTA Enterprise Architecture
OIF	Organisational Interoperability Framework
OMG	Object Management Group
PAS	Patient Administration System
RIM	Reference Information Model
RM-ODP	Reference Model for Open Distributed Processing
SOA	Service-Oriented Architecture
TIF	Technical Interoperability Framework
UML	Unified Modelling Language
WSF	Web Services Framework